Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting

Jérémy Jean

joint work with Patrick Derbez *and* Pierre-Alain Fouque

École Normale Supérieure

Jeremy.Jean@ens.fr

CRYPTO'2012 Rump Session – August 21, 2012

Cipher	Rounds	Data (CP)	Time	Memory	Technique	Reference
AES-128						
AES-192						
AES-256						

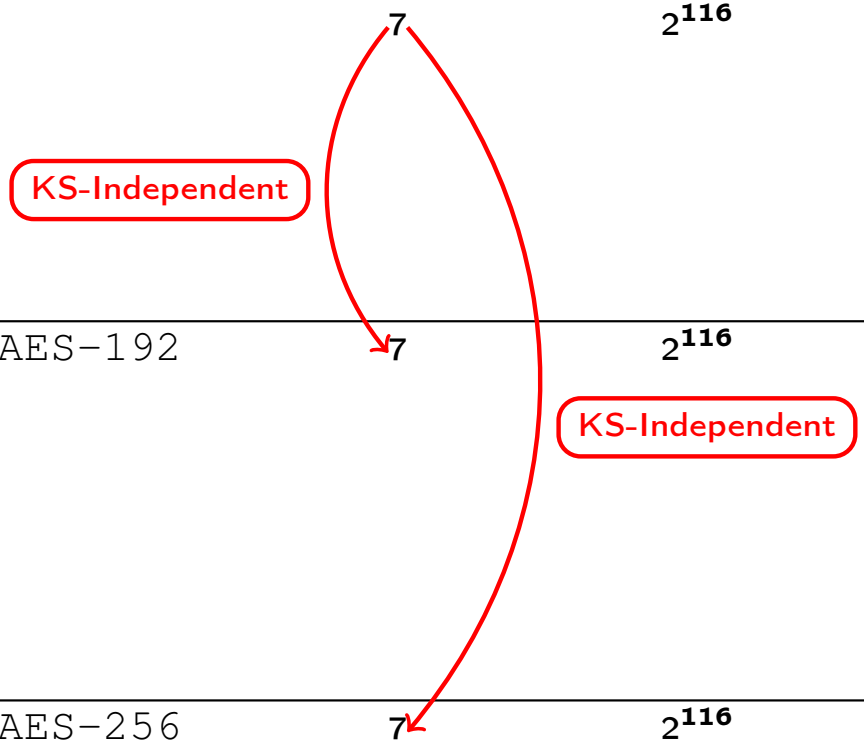
CP: Chosen-plaintext

Cipher	Rounds	Data (CP)	Time	Memory	Technique	Reference
AES-128	7	$2^{112.2}$	$2^{117.2}$	$2^{112.2}$	ID	[LDKK08]
AES-192						
AES-256						

CP: Chosen-plaintext ID: Impossible Differential

[LDKK08] — J. Lu, O. Dunkelman, N. Keller, J. Kim @ Indocrypt 2008

Cipher	Rounds	Data (CP)	Time	Memory	Technique	Reference
AES-128	7	$2^{112.2}$	$2^{117.2}$	$2^{112.2}$	ID	[LDKK08]
	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
AES-192	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
AES-256	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]



CP: Chosen-plaintext ID: Impossible Differential MitM: Meet-in-the-Middle

[DKS10] — O. Dunkelman, N. Keller, A. Shamir @ Asiacrypt 2010

Cipher	Rounds	Data (CP)	Time	Memory	Technique	Reference
AES-128	7	$2^{112.2}$	$2^{117.2}$	$2^{112.2}$	ID	[LDKK08]
	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
AES-192	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
Extension →	8	2^{113}	2^{172}	2^{129}	MitM	[DKS10]
AES-256	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
Extension →	8	2^{113}	2^{196}	2^{129}	MitM	[DKS10]

CP: Chosen-plaintext ID: Impossible Differential MitM: Meet-in-the-Middle

[DKS10] — O. Dunkelman, N. Keller, A. Shamir @ Asiacrypt 2010

Cipher	Rounds	Data (CP)	Time	Memory	Technique	Reference
AES-128	7	$2^{112.2}$	$2^{117.2}$	$2^{112.2}$	ID	[LDKK08]
Improved ID	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	7	$2^{106.2}$	$2^{110.2}$	$2^{90.2}$	ID	[MDRMH10]
AES-192	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	8	2^{113}	2^{172}	2^{129}	MitM	[DKS10]
AES-256	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	8	2^{113}	2^{196}	2^{129}	MitM	[DKS10]

CP: Chosen-plaintext ID: Impossible Differential MitM: Meet-in-the-Middle

[MDRMH10] — H. Mala, M. Dakhilalian, V. Rijmen, M. Modarres-Hashemi @ Indocrypt 2010

Cipher	Rounds	Data (CP)	Time	Memory	Technique	Reference
AES-128	7	$2^{112.2}$	$2^{117.2}$	$2^{112.2}$	ID	[LDKK08]
	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	7	$2^{106.2}$	$2^{110.2}$	$2^{90.2}$	ID	[MDRMH10]
	8	2^{88}	$2^{125.3}$	2^{8}	Bicliques	[BKR11]
	10 (full)	2^{88}	$2^{126.2}$	2^{8}	Bicliques	[BKR11]
AES-192	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	8	2^{113}	2^{172}	2^{129}	MitM	[DKS10]
	9	2^{80}	$2^{188.8}$	2^{8}	Bicliques	[BKR11]
	12 (full)	2^{80}	$2^{189.4}$	2^{8}	Bicliques	[BKR11]
AES-256	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	8	2^{113}	2^{196}	2^{129}	MitM	[DKS10]
	9	2^{120}	$2^{251.9}$	2^{8}	Bicliques	[BKR11]
	14 (full)	2^{40}	$2^{254.4}$	2^{8}	Bicliques	[BKR11]

CP: Chosen-plaintext ID: Impossible Differential MitM: Meet-in-the-Middle

[BKR11] — A. Bogdanov, D. Khovratovich, C. Rechberger @ Asiacrypt 2011

Cipher	Rounds	Data (CP)	Time	Memory	Technique	Reference
AES-128	7	$2^{112.2}$	$2^{117.2}$	$2^{112.2}$	ID	[LDKK08]
	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
Memory improvement	7	$2^{106.2}$	$2^{110.2}$	$2^{90.2}$	ID	[MDRMH10]
	7	2^{105}	2^{99}	2^{90}	MitM	New!
	8	2^{88}	$2^{125.3}$	2^{8}	Bicliques	[BKR11]
	10 (full)	2^{88}	$2^{126.2}$	2^{8}	Bicliques	[BKR11]
AES-192	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	8	2^{113}	2^{172}	2^{129}	MitM	[DKS10]
	9	2^{80}	$2^{188.8}$	2^{8}	Bicliques	[BKR11]
	12 (full)	2^{80}	$2^{189.4}$	2^{8}	Bicliques	[BKR11]
AES-256	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	8	2^{113}	2^{196}	2^{129}	MitM	[DKS10]
	9	2^{120}	$2^{251.9}$	2^{8}	Bicliques	[BKR11]
	14 (full)	2^{40}	$2^{254.4}$	2^{8}	Bicliques	[BKR11]

CP: Chosen-plaintext ID: Impossible Differential MitM: Meet-in-the-Middle

Cipher	Rounds	Data (CP)	Time	Memory	Technique	Reference
AES-128	7	$2^{112.2}$	$2^{117.2}$	$2^{112.2}$	ID	[LDKK08]
	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	7	$2^{106.2}$	$2^{110.2}$	$2^{90.2}$	ID	[MDRMH10]
Tradeoffs	7	2^{105}	2^{99}	2^{90}	MitM	New!
	7	2^{99}	2^{99}	2^{96}	MitM	New!
	8	2^{88}	$2^{125.3}$	2^{8}	Bicliques	[BKR11]
	10 (full)	2^{88}	$2^{126.2}$	2^{8}	Bicliques	[BKR11]
AES-192	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	8	2^{113}	2^{172}	2^{129}	MitM	[DKS10]
	9	2^{80}	$2^{188.8}$	2^{8}	Bicliques	[BKR11]
	12 (full)	2^{80}	$2^{189.4}$	2^{8}	Bicliques	[BKR11]
AES-256	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	8	2^{113}	2^{196}	2^{129}	MitM	[DKS10]
	9	2^{120}	$2^{251.9}$	2^{8}	Bicliques	[BKR11]
	14 (full)	2^{40}	$2^{254.4}$	2^{8}	Bicliques	[BKR11]

CP: Chosen-plaintext ID: Impossible Differential MitM: Meet-in-the-Middle

Cipher	Rounds	Data (CP)	Time	Memory	Technique	Reference
AES-128	7	$2^{112.2}$	$2^{117.2}$	$2^{112.2}$	ID	[LDKK08]
	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	7	$2^{106.2}$	$2^{110.2}$	$2^{90.2}$	ID	[MDRMH10]
	7	2^{105}	2^{99}	2^{90}	MitM	New!
	7	2^{99}	2^{99}	2^{96}	MitM	New!
	8	2^{88}	$2^{125.3}$	2^{8}	Bicliques	[BKR11]
KS-Independent	10 (full)	2^{88}	$2^{126.2}$	2^{8}	Bicliques	[BKR11]
AES-192	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	7	2^{99}	2^{99}	2^{96}	MitM	New!
	8	2^{113}	2^{172}	2^{129}	MitM	[DKS10]
KS-Independent						
	9	2^{80}	$2^{188.8}$	2^{8}	Bicliques	[BKR11]
	12 (full)	2^{80}	$2^{189.4}$	2^{8}	Bicliques	[BKR11]
AES-256	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	7	2^{99}	2^{98}	2^{96}	MitM	New!
	8	2^{113}	2^{196}	2^{129}	MitM	[DKS10]
	9	2^{120}	$2^{251.9}$	2^{8}	Bicliques	[BKR11]
	14 (full)	2^{40}	$2^{254.4}$	2^{8}	Bicliques	[BKR11]

CP: Chosen-plaintext ID: Impossible Differential MitM: Meet-in-the-Middle

Cipher	Rounds	Data (CP)	Time	Memory	Technique	Reference
AES-128	7	$2^{112.2}$	$2^{117.2}$	$2^{112.2}$	ID	[LDKK08]
	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	7	$2^{106.2}$	$2^{110.2}$	$2^{90.2}$	ID	[MDRMH10]
	7	2^{105}	2^{99}	2^{90}	MitM	New!
	7	2^{99}	2^{99}	2^{96}	MitM	New!
	8	2^{88}	$2^{125.3}$	2^{8}	Bicliques	[BKR11]
Extension	10 (full)	2^{88}	$2^{126.2}$	2^{8}	Bicliques	[BKR11]
AES-192	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	7	2^{99}	2^{99}	2^{96}	MitM	New!
	8	2^{113}	2^{172}	2^{129}	MitM	[DKS10]
	8	2^{113}	2^{172}	2^{82}	MitM	New!
Extension	9	2^{80}	$2^{188.8}$	2^{8}	Bicliques	[BKR11]
	12 (full)	2^{80}	$2^{189.4}$	2^{8}	Bicliques	[BKR11]
AES-256	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	7	2^{99}	2^{98}	2^{96}	MitM	New!
	8	2^{113}	2^{196}	2^{129}	MitM	[DKS10]
	8	2^{113}	2^{196}	2^{82}	MitM	New!
	9	2^{120}	$2^{251.9}$	2^{8}	Bicliques	[BKR11]
	14 (full)	2^{40}	$2^{254.4}$	2^{8}	Bicliques	[BKR11]

CP: Chosen-plaintext ID: Impossible Differential MitM: Meet-in-the-Middle

Cipher	Rounds	Data (CP)	Time	Memory	Technique	Reference
AES-128	7	$2^{112.2}$	$2^{117.2}$	$2^{112.2}$	ID	[LDKK08]
	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	7	$2^{106.2}$	$2^{110.2}$	$2^{90.2}$	ID	[MDRMH10]
	7	2^{105}	2^{99}	2^{90}	MitM	New!
	7	2^{99}	2^{99}	2^{96}	MitM	New!
	8	2^{88}	$2^{125.3}$	2^{8}	Bicliques	[BKR11]
	10 (full)	2^{88}	$2^{126.2}$	2^{8}	Bicliques	[BKR11]
AES-192	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	7	2^{99}	2^{99}	2^{96}	MitM	New!
	8	2^{113}	2^{172}	2^{129}	MitM	[DKS10]
Tradeoffs	8	2^{113}	2^{172}	2^{82}	MitM	New!
	8	2^{107}	2^{172}	2^{96}	MitM	New!
	9	2^{80}	$2^{188.8}$	2^{8}	Bicliques	[BKR11]
	12 (full)	2^{80}	$2^{189.4}$	2^{8}	Bicliques	[BKR11]
AES-256	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	7	2^{99}	2^{98}	2^{96}	MitM	New!
	8	2^{113}	2^{196}	2^{129}	MitM	[DKS10]
Tradeoffs	8	2^{113}	2^{196}	2^{82}	MitM	New!
	8	2^{107}	2^{196}	2^{96}	MitM	New!
	9	2^{120}	$2^{251.9}$	2^{8}	Bicliques	[BKR11]
	14 (full)	2^{40}	$2^{254.4}$	2^{8}	Bicliques	[BKR11]

CP: Chosen-plaintext ID: Impossible Differential MitM: Meet-in-the-Middle

Cipher	Rounds	Data (CP)	Time	Memory	Technique	Reference
AES-128	7	$2^{112.2}$	$2^{117.2}$	$2^{112.2}$	ID	[LDKK08]
	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	7	$2^{106.2}$	$2^{110.2}$	$2^{90.2}$	ID	[MDRMH10]
	7	2^{105}	2^{99}	2^{90}	MitM	New!
	7	2^{99}	2^{99}	2^{96}	MitM	New!
	8	2^{88}	$2^{125.3}$	2^{8}	Bicliques	[BKR11]
	10 (full)	2^{88}	$2^{126.2}$	2^{8}	Bicliques	[BKR11]
AES-192	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	7	2^{99}	2^{99}	2^{96}	MitM	New!
	8	2^{113}	2^{172}	2^{129}	MitM	[DKS10]
	8	2^{113}	2^{172}	2^{82}	MitM	New!
	8	2^{107}	2^{172}	2^{96}	MitM	New!
	9	2^{80}	$2^{188.8}$	2^{8}	Bicliques	[BKR11]
	12 (full)	2^{80}	$2^{189.4}$	2^{8}	Bicliques	[BKR11]
AES-256	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	7	2^{99}	2^{98}	2^{96}	MitM	New!
	8	2^{113}	2^{196}	2^{129}	MitM	[DKS10]
	8	2^{113}	2^{196}	2^{82}	MitM	New!
	8	2^{107}	2^{196}	2^{96}	MitM	New!
	9	2^{120}	$2^{251.9}$	2^{8}	Bicliques	[BKR11]
	9	2^{120}	2^{203}	2^{203}	MitM	New!
	14 (full)	2^{40}	$2^{254.4}$	2^{8}	Bicliques	[BKR11]

Extension & Tradeoffs

CP: Chosen-plaintext ID: Impossible Differential MitM: Meet-in-the-Middle

Cipher	Rounds	Data (CP)	Time	Memory	Technique	Reference
AES-128	7	$2^{112.2}$	$2^{117.2}$	$2^{112.2}$	ID	[LDKK08]
	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	7	$2^{106.2}$	$2^{110.2}$	$2^{90.2}$	ID	[MDRMH10]
	7	2^{105}	2^{99}	2^{90}	MitM	New!
	7	2^{99}	2^{99}	2^{96}	MitM	New!
	8	2^{88}	$2^{125.3}$	2^{8}	Bicliques	[BKR11]
	10 (full)	2^{88}	$2^{126.2}$	2^{8}	Bicliques	[BKR11]
AES-192	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	7	2^{99}	2^{99}	2^{96}	MitM	New!
	8	2^{113}	2^{172}	2^{129}	MitM	[DKS10]
	8	2^{113}	2^{172}	2^{82}	MitM	New!
	8	2^{107}	2^{172}	2^{96}	MitM	New!
	9	2^{80}	$2^{188.8}$	2^{8}	Bicliques	[BKR11]
	12 (full)	2^{80}	$2^{189.4}$	2^{8}	Bicliques	[BKR11]
AES-256	7	2^{116}	2^{116}	2^{116}	MitM	[DKS10]
	7	2^{99}	2^{98}	2^{96}	MitM	New!
	8	2^{113}	2^{196}	2^{129}	MitM	[DKS10]
	8	2^{113}	2^{196}	2^{82}	MitM	New!
	8	2^{107}	2^{196}	2^{96}	MitM	New!
	9	2^{120}	$2^{251.9}$	2^{8}	Bicliques	[BKR11]
	9	2^{120}	2^{203}	2^{203}	MitM	New!
	14 (full)	2^{40}	$2^{254.4}$	2^{8}	Bicliques	[BKR11]

CP: Chosen-plaintext ID: Impossible Differential MitM: Meet-in-the-Middle

Soon on the ePrint.

Thanks for listening!

Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger.

Biclique Cryptanalysis of the Full AES.

In Dong Hoon Lee and Xiaoyun Wang, editors, Asiacrypt, volume 7073 of *Lecture Notes in Computer Science*, pages 344–371. Springer, 2011.

Orr Dunkelman, Nathan Keller, and Adi Shamir.

Improved Single-Key Attacks on 8-Round AES-192 and AES-256.

In Masayuki Abe, editor, Asiacrypt, volume 6477 of *Lecture Notes in Computer Science*, pages 158–176. Springer, 2010.

Jiqiang Lu, Orr Dunkelman, Nathan Keller, and Jongsung Kim.

New Impossible Differential Attacks on AES.

In Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, editors, Indocrypt, volume 5365 of *Lecture Notes in Computer Science*, pages 279–293. Springer, 2008.

Hamid Mala, Mohammad Dakhilalian, Vincent Rijmen, and Mahmoud Modarres-Hashemi.

Improved Impossible Differential Cryptanalysis of 7-Round AES-128.

In Guang Gong and Kishan Chand Gupta, editors, Indocrypt, volume 6498 of *Lecture Notes in Computer Science*, pages 282–291. Springer, 2010.