Make AES great again!

Nathan Keller
Bar Ilan University

Joint work with Achiya Bar-On, Orr Dunkelman, Eyal Ronen, and Adi Shamir

Block Ciphers

- The most common symmetric key primitive.
- Maps an b-bit plaintext P to an b-bit ciphertext C, using an n-bit key K.

Reduced-round variants

- Most block ciphers are iterative, i.e., composed of similar small units called rounds.
- We consider attacks not only on the full cipher but also on reduced-round variants.
- **Motivation:**
  - Understand security margin.
  - Attacks tend to improve.
  - Reduced-round variants used in other primitives.

A "good" block cipher?

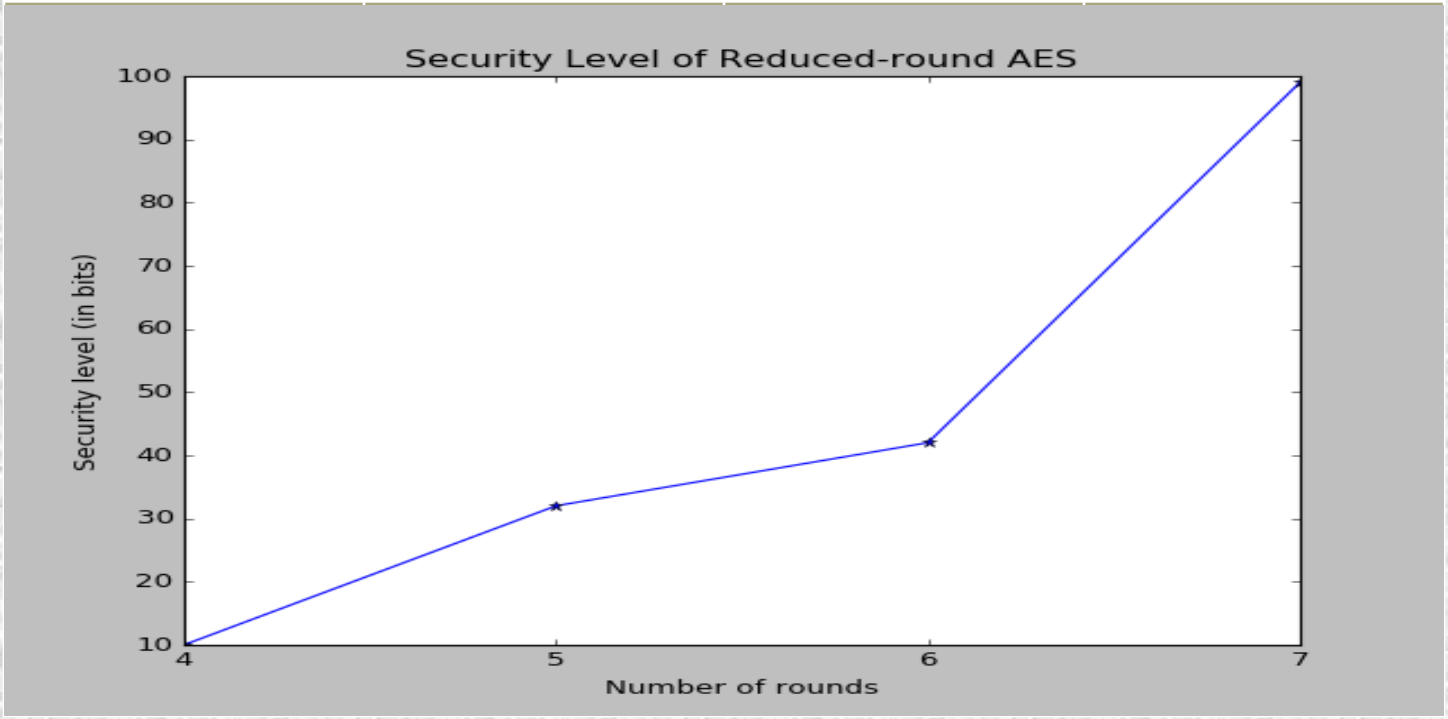
- We define the security level of a variant as log of the complexity of the best attack on it.
  - "For a good block cipher, the security level should grow exponentially with the number of rounds" (folclore)
- A bad block cipher: DES
  - Security grows only linearly in the number of rounds, due to differential and linear cryptanalysis.

Is AES a "good" block cipher?

Number of rounds	Security level (in bits)	Best attack	Year of publication
4	10	2^{10}	1996
5	32	2^{32}	2000
6	42	2^{42}	2000
7	99	2^{99}	2013
8	128	none	-

- Does security grow exponentially with the number of rounds?

Is AES a "good" block cipher?



- Does security grow exponentially with the number of rounds?

No!

Our new result

- 5-round AES used as a component in: WEM, Hound, ELmD

- Best previous attacks on 5-round AES:

Technique	Complexity	Year
Square	2^{32}	2000
Imp. Differential	2^{32}	2001
Yoyo	2^{32}	2017
Mixture Differential	2^{32}	2018

Our new result

- 5-round AES used as a component in: WEM, Hound, ELmD

- Best previous attacks on 5-round AES:

Technique	Complexity	Year
Square	2^{32}	2000
Imp. Differential	2^{32}	2001
Yoyo	2^{32}	2017
Mixture Differential	2^{32}	2018

Our attack: 2^{22}

We make AES great again!

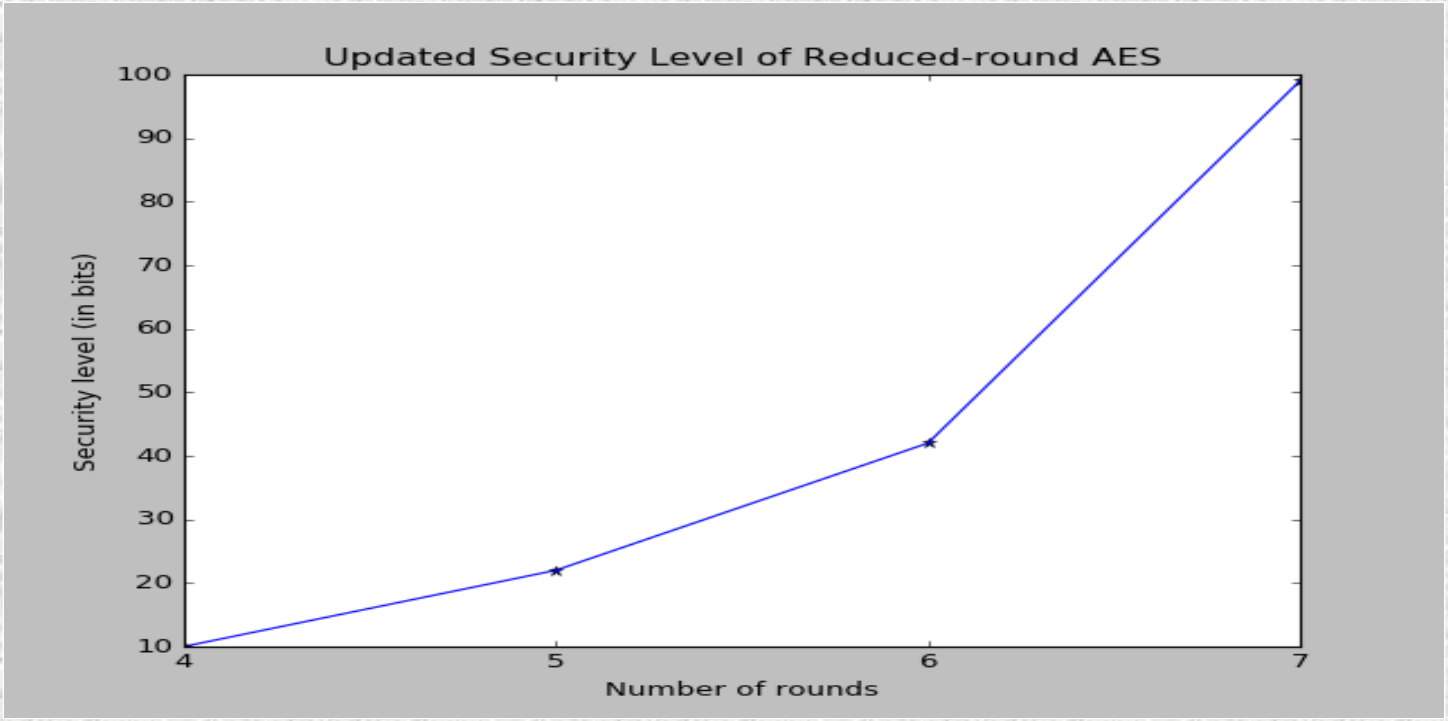
- Updated security level of reduced-round AES:

Number of rounds	Security level (in bits)	Best attack	Year of publication
4	10	2^{10}	1996
5	22	2^{22}	2018
6	42	2^{42}	2000
7	99	2^{99}	2013
8	128	none	-

- Does security grow exponentially with the number of rounds?

We make AES great again!

- Updated security level of reduced-round AES:



- Does security grow exponentially with the number of rounds?

Yes!

Thanks for listening!