Diving Deep into the Preimage Security of AES-like Hashing

Shiyao Chen, Jian Guo, Eik List, Danping Shi, **Tianyu Zhang**[*]

[*]Nanyang Technological University, Singapore

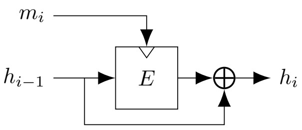
27 May 2024

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

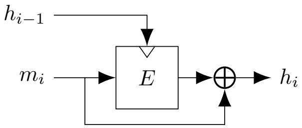
Outline

Construct hash functions based on block ciphers

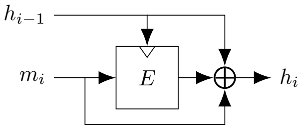
1. Convert an encryption function E to a compression function CF with a PGV mode



Davies-Meyer (DM)

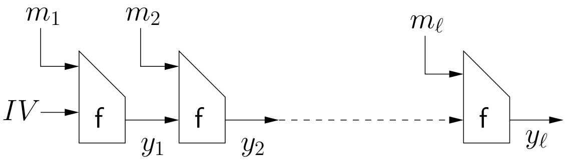


Matyas-Meyer-Oseas (MMO)



Miyaguchi-Preneel (MP)

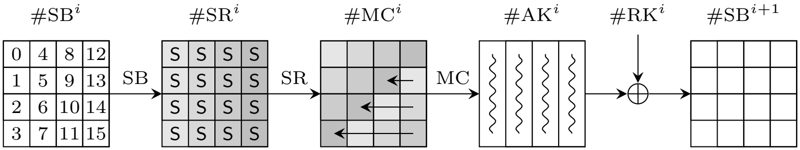
2. Then iterate the CF following the Merkle-Damgård construction



NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

The AES round function

AES is selected by NIST in 2001 from the Rijndael block cipher family.



An encryption state of AES is organized as a $4 * 4$ grid of bytes. An AES round consists of the following operations:

- SubBytes (SB): a non-linear byte-wise substitution (S-box)
- ShiftRows (SR): a cyclic left shift on the *i*-th row by *i* bytes
- MixColumns (MC): a column-wise left multiplication of an MDS matrix
- AddRoundKey (AK): a bitwise XOR of the round key to the state

AES-like Hashing

The outstanding security of AES has inspired many designs.

Hash functions with a compression function **based on** or **similar to** the AES round function is refered to as AES-like hash functions or AES-like hashing.

Examples include:

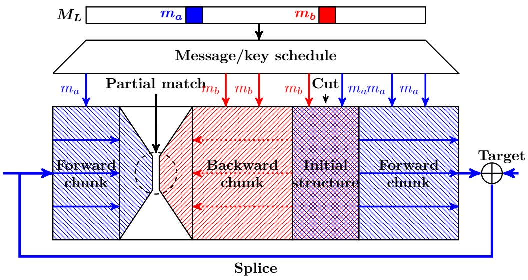
- AES-MMO (standard in the Zigbee protocol suite and ISO/IEC standard)
- Whirlpool (ISO/IEC standard)
- Streebog (ISO/IEC standard)
- Grøstl
- Saturnin
- etc.

Outline

Meet-in-the-Middle attacks

In a series of works, Aoki and Sasaki proposed the Meet-in-the-Middle (MITM) attack on hash functions. An MITM attack is orchestrated as follows:

- For $2^{n-d_b-d_r}$ values of $M_L/\{m_a, m_b\}$:
  - For 2^{d_b} values of m_a, compute forward to the matching point and save in a table T^+;
  - For 2^{d_r} values of m_b, compute backward and save in a table T^-;
  - If find a match between T^+, T^-:
  - Test whether a full match and return the preimage;



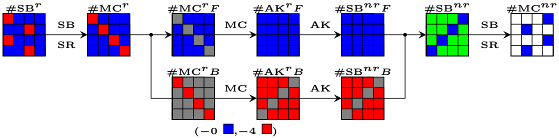
Total complexity:

$$2^{(n-d_b-d_r)} \cdot (2^{d_b} + 2^{d_r} + 2^{d_b+d_r-d_M}) \simeq 2^{n-\min(d_b,d_r,d_M)}.$$

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Byte classification in MITM attacks

- a forward neutral byte, represented by ■ (blue)
- a backward neutral byte, represented by ■ (red)
- a constant byte, represented by ■ (grey)
- an unknown byte, represented by □
- a superposition byte, represented by ■ (green), value of which is the sum of its forward and backward neutral components: $v = v^{+} \oplus v^{-}$.
  - a superposition byte is preserved through all **linear operations**
  - after the **nonlinear operations** (*e.g.*, an S-box), a superposition byte becomes unknown



Outline

Exploiting the algebraic structure of AES S-box

At Asiacrypt 2023, Zhang *et al.* observed the non-linear layer of the AES S-box has the following decomposition:

$$x^{254} = (x^{17})^{14} \cdot x^{16}$$

The decomposition has the following properties:

- x^{17} has 15 possible non-zero possible values, 16 in total
- x^{16} is linear, as x^2 over $\mathbb{F}_{2^8}$ is linear

However, the observation did not lead to better results on AES, quoting their words:

This linearizes the non-linear layer of AES, but unfortunately, no attacks better than the current state-of-the-art has been found based on this fact.

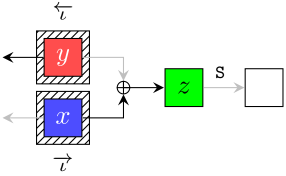
Linearizating AES S-box in MITM attacks

We generalize the observation to the superposition bytes:

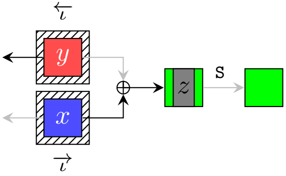
$$v^{254} = (v^{+} + v^{-})^{254} = ((v^{+} + v^{-})^{17})^{14} \cdot (v^{+} + v^{-})^{16}$$
$$= (H(v^{+}, v^{-}))^{14} \cdot ((v^{+})^{16} + (v^{-})^{16})$$

Thus, a superposition byte can be **preserved** after an AES S-box by

- an enumeration over the pool of $|\{H(z) = z^{17} : z \in \mathbb{F}_{2^8}\}| = 16$ hints, and
- an efficient checking, as it only requires local information (unlike GnD)



Orignal superposition



Guessing part of the superposition

Outline

1. Backgound
   - AES-like hashing
   - Meet-in-the-Middle Attack
2. Advanced Techniques for MITM Attacks
   - S-box Linearization (**LIN**)
   - Distributed Initial Structures (**DIS**)
   - Structual Similarity (**SIM**)
3. Applications
   - AES and Rijndael
   - Whirlpool and Streebog
4. Conclusion

Choice of initial states

In previous MITM attacks, one intuitively choose

- a full state $\overleftrightarrow{S}^{\mathtt{ENC}}$ in the encryption function and
- a full state $\overleftrightarrow{S}^{\mathtt{KSA}}$ in the key schedule

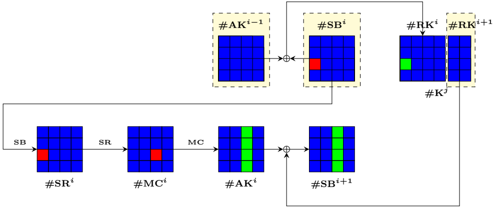
as initial states to allocate ■, ■, or ■ (no superpositions).

In essence, the initial states in MITM attacks are some **independent** intermediate values where we distribute initial DoFs for forward and backward computations.

In this work, we introduce the distributed initial structure (**DIS**), which:

- remove the artificial constraint on initial states
- allow more combinations of the initial states

An example of **DIS** in AES-192



We will distribute initial DoFs in

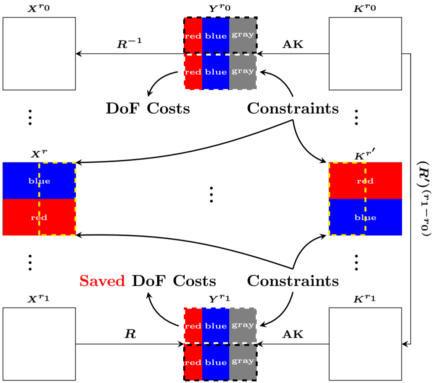
- $\#\mathrm{AK}^{i-1}$
- $\#\mathrm{SB}^{i}$
- the rightmost two columns of $\#\mathrm{K}^{j}$

The effect of **DIS** includes:

- $\#\mathrm{K}^{j}$ can be expressed and used as $\overleftrightarrow{S}^{\mathtt{KSA}}$ for further key schedule propagations
- Thus, superpositions are now allowed in $\overleftrightarrow{S}^{\mathtt{KSA}}$, and
- more superposition information can be preserved in the AES key schedule

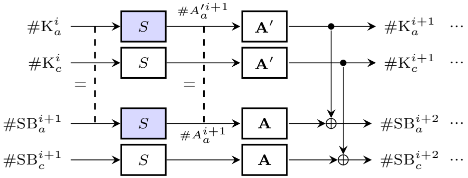
Outline

Related constraints at AddRoundKey



- Previous models consider constraints incurred at AK in different rounds as **independent**
- However, the constraints may be added to the same DoF source in multiple rounds
- In other words, the constraints can be **related**

Exploiting **SIM** in Whirlpool and Streebog



- The encryption and the key schedule share the same round function
- If $\#\mathrm{AK}_a^i$ is 0, then $\#\mathrm{SB}_a^{i+1} = 0 \oplus \#\mathrm{K}_a^i = \#\mathrm{K}_a^i$
- After the same sets of operations, $\#\mathrm{SB}_a^{i+2}$ should be constant after XOR
- Previous models may invoke unnecessary costs to have constants in $\#\mathrm{SB}_a^{i+2}$

Outline

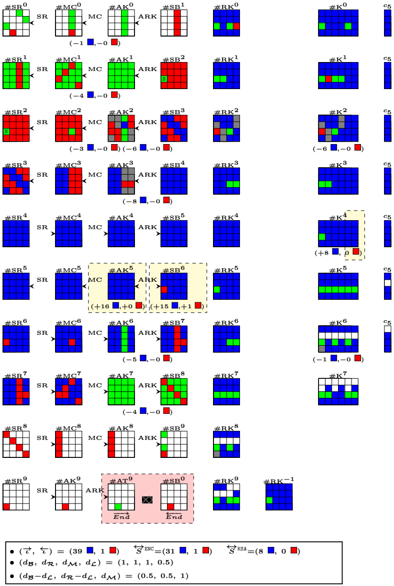
1. Backgound
   - AES-like hashing
   - Meet-in-the-Middle Attack
2. Advanced Techniques for MITM Attacks
   - S-box Linearization (**LIN**)
   - Distributed Initial Structures (**DIS**)
   - Structual Similarity (**SIM**)
3. Applications
   - AES and Rijndael
   - Whirlpool and Streebog
4. Conclusion

Preimage Attacks

Cipher (target)	#Rounds	T_1 †	T_2 ‡	Memory	Essential technique(s)	References
AES-192 (Hash)	8/12	2^{112}	2^{116}	2^{16}	MITM	[BDGWZ19]
	8/12	2^{100}	2^{115}	2^{96}	**LIN**, **DIS**, BiDir	This work
	9/12	2^{120}	2^{125}	–	MILP	[BDGLSSW21]
	9/12	2^{112}	2^{121}	–	BiDir	[BGST22]
	10/12	2^{124}	2^{127}	2^{124}	**LIN**, **DIS**, BiDir	This work
Rijndael-192/192 (Hash)	9/12	2^{184}	2^{189}	–	BiDir	[Zha23]
	9/12	2^{180}	2^{187}	2^{180}	**LIN**, BiDir	This work
Rijndael-192/256 (Hash)	9/12	2^{168}	2^{181}	–	BiDir	[Zha23]
	10/12	2^{188}	2^{191}	2^{180}	**LIN**, BiDir	This work

† T_1 is the time complexity of the pseudo-preimage attack on compression function.

‡ T_2 is the time complexity of the preimage attack on hash function.



- The **first** 10-round preimage/pseudo-preimage attack on `AES-192`
- Linearizing an S-box from $\#\mathrm{SR}^2$ to $\#\mathrm{SB}^2$
- Distributing initial states to $\#\mathrm{AK}^{i-1}$, $\#\mathrm{SB}^{i}$ and the rightmost two columns of $\#\mathrm{K}^{j}$
- 2^{124} for pseudo-preimage and 2^{127} for preimage
  - different from biclique attacks
  - not reduced to S-box level evaluation

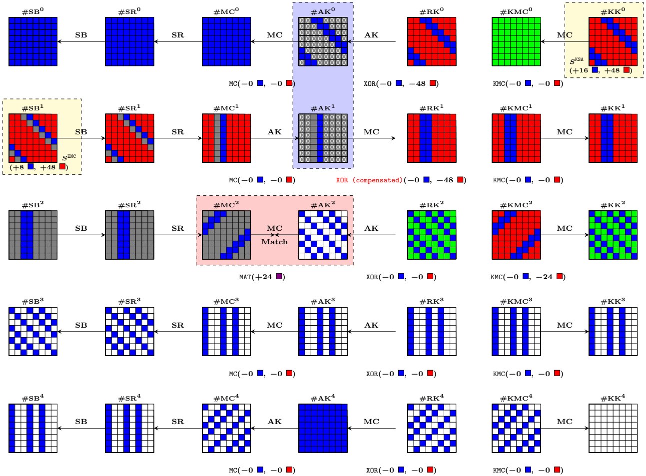
NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Outline

1. Backgound
   - AES-like hashing
   - Meet-in-the-Middle Attack
2. Advanced Techniques for MITM Attacks
   - S-box Linearization (**LIN**)
   - Distributed Initial Structures (**DIS**)
   - Structual Similarity (**SIM**)
3. Applications
   - AES and Rijndael
   - Whirlpool and Streebog
4. Conclusion

Preimage Attacks						
Cipher (target)	#Rounds	T_1 †	T_2 ‡	Memory	Essential technique(s)	References
Whirlpool (Hash)	5/10	2^{416}	2^{448}	2^{96}	Dedicated method	[SWWW12]
	5/10	2^{352}	2^{433}	2^{160}	BiDir, MulAK	[BGST22]
	5/10	2^{320}	2^{417}	$O(1)$	**SIM**, BiDir	This work
	6/10	2^{448}	2^{481}	2^{256}	Dedicated method, GnD	[SWWW12]
	6/10	2^{440}	2^{477}	2^{192}	GnD	[BGST22]
	6/10	2^{416}	2^{465}	2^{288}	**SIM**, BiDir, GnD	This work
	7/10	2^{480}	2^{497}	2^{128}	GnD, MulAK	[BGST22]
	7.75/10	2^{480}	2^{497}	2^{256}	**SIM**, BiDir, GnD	This work

Collision Attacks					
Cipher (target)	#Rounds	Time	Memory	Essential technique(s)	References
Whirlpool (Hash)	4.5/10	2^{120}	2^{16}	Rebound	[MRST09]
	4.5/10	2^{64}	2^{16}	Rebound	[LMSRR15]
	5/10	2^{120}	2^{64}	Super-SBox	[LMRRS09; GP10]
	5.5/10	2^{184-s}	2^{s}	Rebound	[LMSRR15]
	6/10	2^{228}	2^{228}	Quantum	[HS20]
	6/10	2^{248}	2^{248}	MILP, MITM	[DHSLWH21]
	6/10	2^{240}	2^{240}	New MILP model, MITM	This work
	6.5/10	2^{240}	2^{240}	New MILP model, MITM	This work



- $(\overrightarrow{\iota}, \overleftarrow{\iota})$ = (8+16)=24, (48+0)=48
- $(d_{\mathcal{B}}, d_{\mathcal{R}}, d_{\mathcal{M}}, g_{\mathcal{B}}, g_{\mathcal{R}}, g_{\mathcal{BR}})$ = (+24, +24, +24, +0, +0, +0)
- $(d_{\mathcal{B}}-g_{\mathcal{R}}, d_{\mathcal{R}}-g_{\mathcal{B}}, d_{\mathcal{M}}-g_{\mathcal{B}}-g_{\mathcal{R}}-g_{\mathcal{BR}})$ = (24, 24, 24)

- DoF compensation at round 1
- **Same color** match at round 3
- 2^{32} times (pseudo-preimage) and 2^{16} times (preimage) improvements than previous best attack
- Reduce memory cost to $O(1)$ (compared to previous best attack with 2^{160})

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Preimage Attacks

Cipher (target)	#Rounds	T_1 †	T_2 ‡	Memory	Essential technique(s)	References
Streebog-512 (Compression)	7.5/12	2^{496}	–	2^{64}	Dedicated method	[MLHL15]
	7.5/12	2^{441}	–	2^{192}	GnD, MulAK	[HDSZHW22]
	7.5/12	2^{433}	–	2^{177}	**SIM**, GnD	This work
	8.5/12	2^{481}	–	2^{288}	GnD, MulAK	[HDSZHW22]
	8.5/12	2^{481}	–	2^{129}	**SIM**, GnD	This work
Streebog-512 (Hash)	7.5/12	–	2^{496}	2^{64}	Dedicated method	[MLHL15]
	7.5/12	–	$2^{478.25}$	2^{256}	MITM + Multi-collision¶	[HDSZHW22]
	7.5/12	–	$2^{474.25}$	2^{256}	MITM + Multi-collision	This work
	8.5/12	–	$2^{498.25}$	2^{288}	MITM + Multi-collision	[HDSZHW22]
	8.5/12	–	$2^{498.25}$	2^{256}	MITM + Multi-collision	This work

¶ The attack on the compression function of Streebog is converted into a preimage attack on its hash function using the technique from [AY14].

Conclusion

In this paper, we

- introduced three new advanced techniques into MITM: S-box Linearization (**LIN**), Distributed Initial Structures (**DIS**) and Structual Similarity (**SIM**)
- furnished the MITM framework and constructed more efficient MILP-based model
- found first 10-round MITM preimage/pseudo-preimage attacks on `AES-192` hashing
- improved MITM preimage/pseudo-preimage and/or collision attacks on `Whirlpool` and `Streebog`

For more details, please refer to our paper :)

`https://eprint.iacr.org/2024/300`

TYFL!