Tiaoxin-346

Ivica Nikolić

NTU, Singapore

Initial Goals

- Fast(est) on AES-NI platforms
- Secure in nonce-respecting

How to Use AES-NI

AES-NI provides one round of AES.
But, the real efficiency comes only with proper use.
Example: Both, AES-CBC and AES-CTR rely on 10-round AES, but the second is much faster.

Parallel calls to AES rounds

Faster, Faster

There is (almost) a theoretical limit of how fast AES-design can be
Based on 4-round AES, cannot go faster than 4/16=0.25 c/b

Challenge the use of 4-round AES

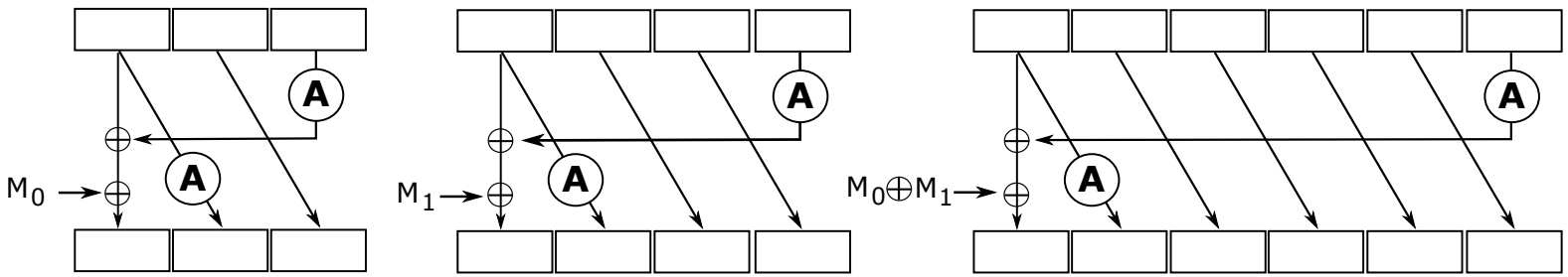
Security of AE

Attacker is rather limited (without exotic attack frameworks)

- Main threat: differential trails that start and end with zero difference (aka LOCAL on ALE)
- Other big threats: state recovery, correlation
- Many other 'standard' threats

Tiaoxin-346

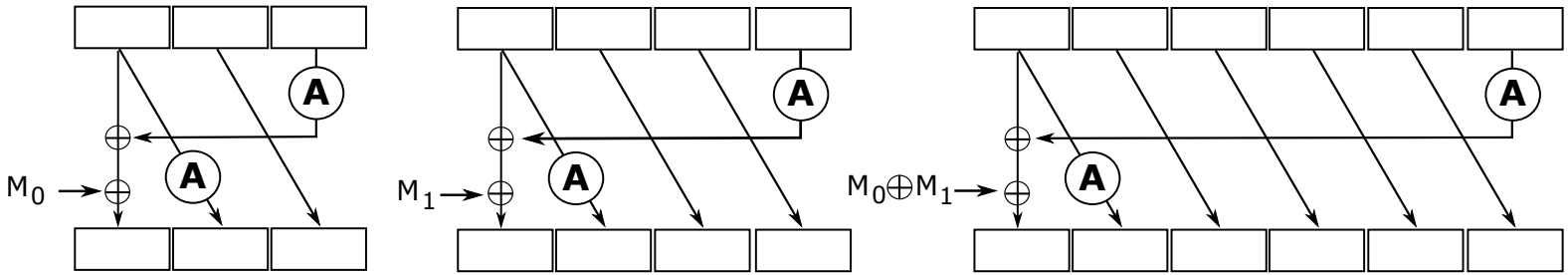
Round function



- each word is 128 bits
- three states of 3,4,6 words (thus Tiaoxin-346)
- no mixing between states (for easier analysis)

Tiaoxin-346 - Speed

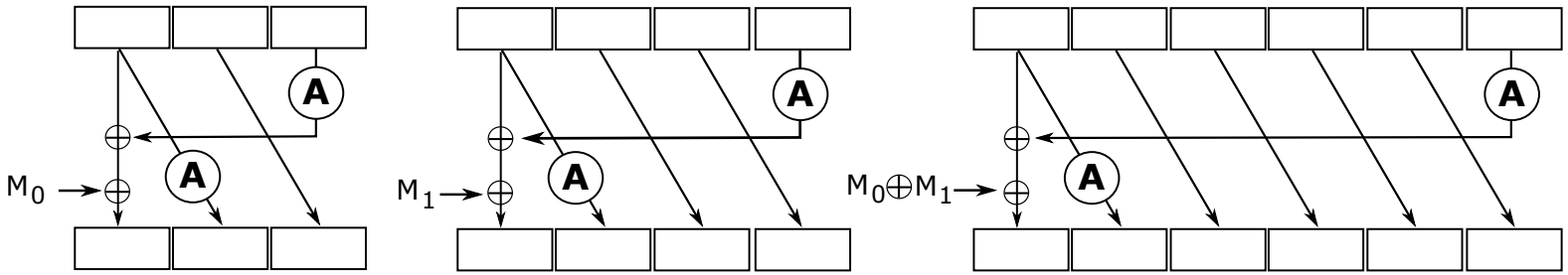
Round function



- 6 AES round to process 2 message words
- 3 AES rounds per 16 bytes **(below the magic bound of 4 AES rounds)**
- All 6 calls parallelizable
- Will achieve max speed when latency of AES-NI round is **6 and below**

Tiaoxin-346 - Security

Round function

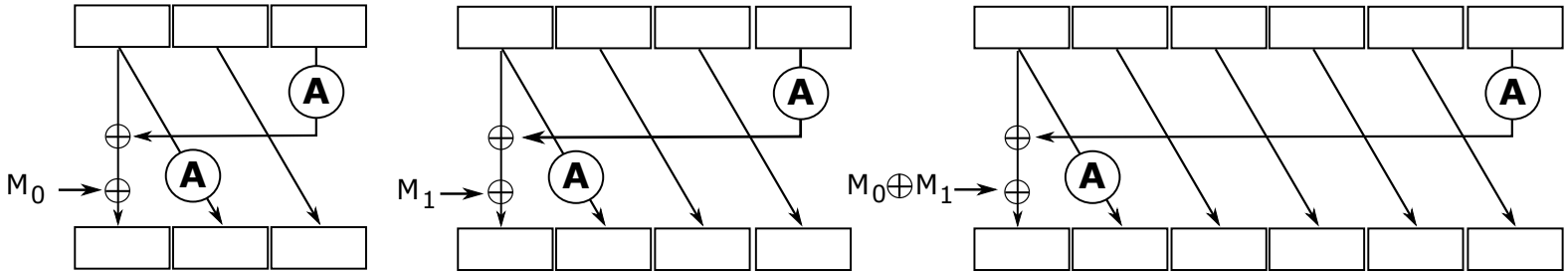


Security against LOCAL attack

- Instead of basing it on property of **one** 4-round diff. trail, it is based on **many 2-round trails**
- State sizes (of 3,4,6 words) were chosen to resist this attack
- Sizes are minimal
- Resistance shown with automatic search tools

Tiaoxin-346 - Security

Round function



Security against state recovery, correlations

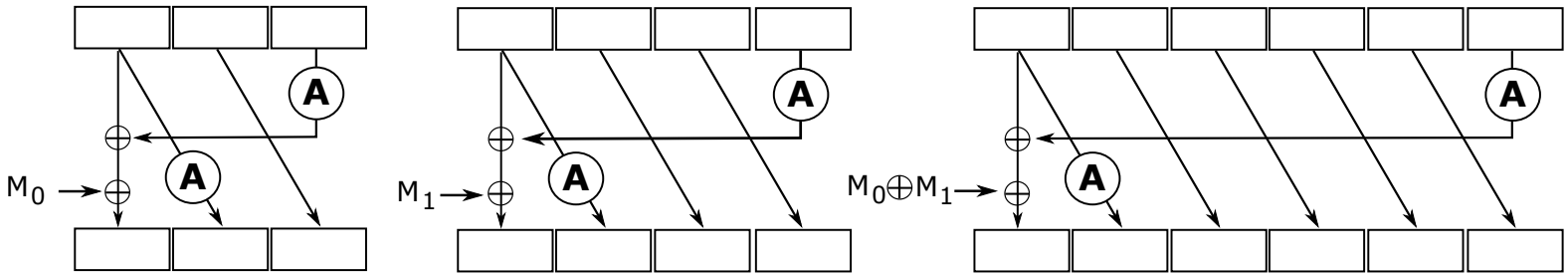
- Ciphertexts depend on several words of the 3 states:

$$C^0 = T_3[0] \oplus T_3[2] \oplus T_4[1] \oplus (T_6[3] \,\&\, T_4[3])$$
$$C^1 = T_6[0] \oplus T_4[2] \oplus T_3[1] \oplus (T_6[5] \,\&\, T_3[2])$$

- Only 2 words of output per round (the state has 13 words)
- Have to take outputs of 6.5 rounds in order to recover the whole state

Tiaoxin-346 - Security

Round function



Security against other attacks

- Initialization composed of 15 rounds protects against related-key (IV) differential attacks
- Finalization composed of 20 rounds protects against other (non-LOCAL) attacks
- Use of two constants provides resistance against attacks exploiting symmetry

Tiaoxin-346 - Summary

- AES-NI optimized scheme
- Uses only 3 AES round per 16-byte message
- Has a large state (64 bits larger than Keccak)
- Secure in nonse-respecting

All this makes Tiaoxin-346 candidate for
use case 2: high-performance applications