




AEGIS

A Fast Authenticated Encryption Algorithm

Hongjun Wu, Bart Preneel

Nanyang Technological University, Katholieke Universiteit Leuven

- 
- Classification of Authenticated Encryption
 - AEGIS
 - Design rationale
 - Specification
 - Security
 - Performance
 - Comparison with other AE algorithms



Classification of Authenticated Encryption

- Common practice to protect messages
 - Encryption + Authentication
- One way to classify authentication encryption is based on nonce:
 - Whether nonce is needed?
 - Whether the security is sensitive to nonce reuse?

Classification of AE based on nonce

- Two main types of encryption based on nonce
 - block cipher in CBC mode
 - with nonce: secure
 - nonce reuse: secure for many applications (BitLocker)
 - synchronous stream cipher
 - with nonce: secure
 - nonce reuse: insecure

Classification of AE based on nonce

- Two main types of MACs
 - MAC without nonce (fixed nonce)
 - HMAC, CMAC, Pelican MAC, PMAC ...
 - Reliable, but not the most efficient
 - MAC with nonce
 - UMAC (VMAC, Poly1305-AES)
 - Nonce reuse: insecure

Classification of AE based on nonce

- Two main types of AE
 - Security not sensitive to nonce reuse
 - One pass AE: A and E not sensitive to nonce reuse
 - Example: CBC + HMAC
 - Two pass AE: A not sensitive to nonce reuse
 - Security sensitive to nonce reuse
 - One pass AE: A or E sensitive to nonce reuse
- AEGIS
 - Security sensitive to nonce reuse

Design Rationale of AEGIS

- Design a fast AE algorithm to protect internet communication
 - reduce packet delay due to authentication/encryption at a busy server
 - TLS, SSH (or VPN)
 - easy to avoid nonce re-use for each session key
- AEGIS based on nonce reuse (more efficient)



Design Rationale of AEGIS

- AES new instruction set (AES-NI)
 - Intel Westmere
 - 6 clock cycles/AESNI instruction, 3-stage pipeline
 - Intel Sandy Bridge
 - 8 clock cycles/AESNI instruction, 8-stage pipeline
 - 8-stage pipeline does not benefit much CBC encryption at a sever (different session keys are used)
- AEGIS is to use several parallel AES instructions



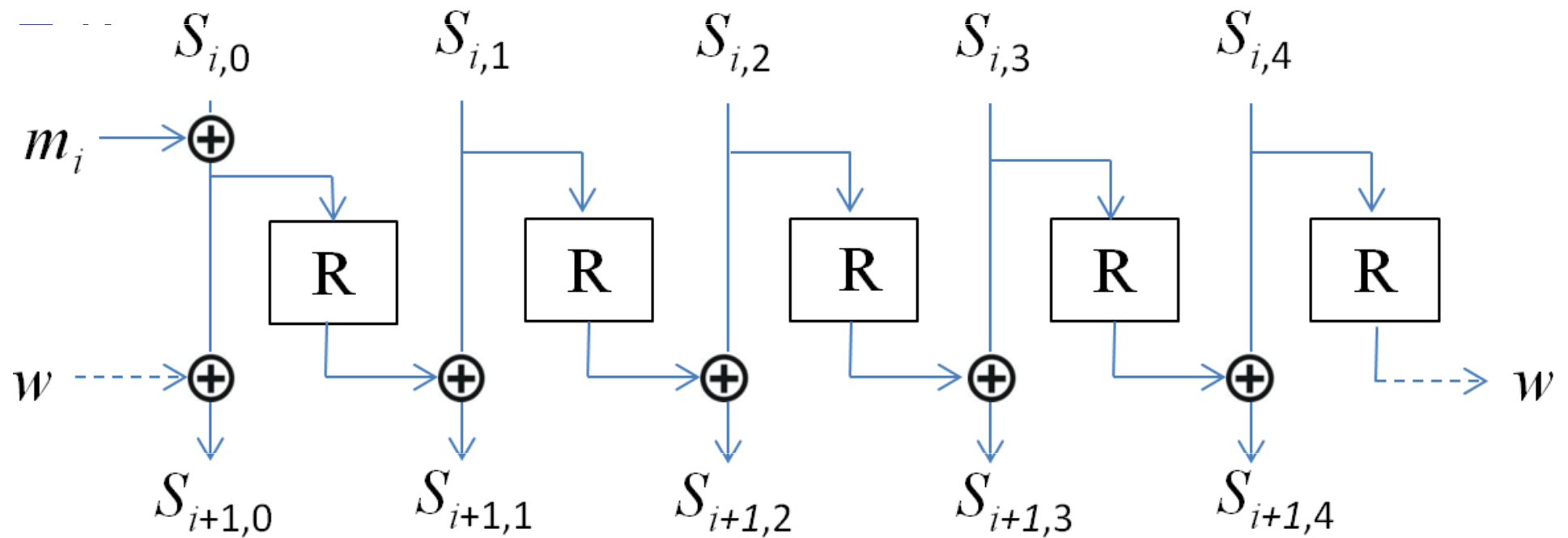
Design Rationale of AEGIS

- Partly motivated by Pelican MAC
 - Pelican MAC (using AES round functions)
 - 128-bit secret state
 - XOR a 128-bit message block with state, pass through 4 AES rounds (no round key),
.....
 - Easy to analyze, strong

Design Rationale of AEGIS

- Partly motivated by Pelican MAC (cont.)
 - How to convert Pelican MAC to an AE algorithm?
 - Save intermediate values between round functions to improve computing efficiency
 - Generate keystream from the state
 - AEGIS-128: 5×128 -bit state
 - AEGIS-256: 6×128 -bit state
 - Large state here is mainly for the security of encryption

Specifications of AEGIS-128





Security Requirements of AEGIS

- Each key should be randomly generated
- Each key and nonce pair be used only once
- If verification fails, the decrypted message and wrong message authentication tag should not be given as output

Security Claims of AEGIS

- Secret key cannot be recovered faster than exhaustive key search
- Success rate of a forgery attack is 2^t
 - t is tag size
- The state cannot be recovered faster than exhaustive key search
 - if forgery attempt is not allowed for multiple times (or less than 2^t times) for each key and nonce pair

Performance of AEGIS

Intel Sandy Bridge Core-i5

	1B	16B	64B	512B	1024B	4096B	65536B	IPI ^a
AEGIS-128(EA ^b)	149	9.20	2.74	0.91	0.79	0.67	0.64	1.03
AEGIS-128(DV ^c)	175	9.30	2.85	0.99	0.83	0.69	0.64	1.08
AEGIS-256(EA)	228	12.54	3.64	1.08	0.88	0.71	0.66	1.19
AEGIS-256(DV)	238	12.88	4.00	1.16	0.93	0.76	0.71	1.27

Intel Sandy Bridge Core-i7

AES-128-CTR

OCB

GCM

CCM

0.66

0.87

2.95

5.14

Performance of AEGIS

- On other platforms

- AEGIS-128: 5 AES round functions/16 bytes
 - AES-128: 10 AES round functions/16 bytes
- ⇒ The computational cost of AEGIS is less than half of OCB, GCM, CCM

Performance of AEGIS-MAC

	1B	16B	64B	512B	1024B	4096B	65536B	IPI ^a
AEGIS-128(EA ^b)	149	9.20	2.74	0.91	0.79	0.67	0.64	1.03
AEGIS-128(DV ^c)	175	9.30	2.85	0.99	0.83	0.69	0.64	1.08
AEGIS-256(EA)	228	12.54	3.64	1.08	0.88	0.71	0.66	1.19
AEGIS-256(DV)	238	12.88	4.00	1.16	0.93	0.76	0.71	1.27
AEGIS-128-5-MAC-wn	148	9.19	2.67	0.82	0.69	0.59	0.56	0.95
AEGIS-128-4-MAC-wn	149	9.33	2.65	0.82	0.70	0.59	0.56	0.95
AEGIS-128-4-MAC-won	182	11.41	3.17	0.88	0.72	0.60	0.56	1.00
AEGIS-128-8-MAC-wn	197	12.2	2.88	0.64	0.48	0.37	0.32	0.77
AEGIS-128-8-MAC-won	234	14.56	3.56	0.73	0.52	0.38	0.33	0.85
AEGIS-256-6-MAC-wn	228	12.40	3.48	0.98	0.77	0.62	0.56	1.08

Intel Sandy Bridge Core-i5

Performance of AEGIS

- Compare with the DIAC two-pass scheme
 - Scheme of Aoki et al, 2 cycles/byte
 - AEGIS-128 in two-pass
 - $0.67+0.60 = 1.27$ cycles/byte for 4096-byte message
 - or $0.67+0.38 = 1.05$ cycles/byte
 - faster than the Aoki et al.'s scheme
 - Reason: Pelican MAC + CTR
 - Pelican MAC uses only one pipeline stage.

Conclusion

■ AEGIS

- targeting platform with AES-NI
- Simple design
- Efficient for internet packets
- Strong security



Thank you!

Q & A