AEGIS A Fast Authenticated Encryption Algorithm

Hongjun Wu Bart Preneel

Nanyang Technological University KU Leuven and iMinds



AEGIS: A shield carried by Athena and Zeus

Different Design Approaches:



AEGIS: Main features

- Fast
 - AEGIS-128L is 0.30 clock cycles/byte on Haswell (16KB messages)
 - Fully use the pipeline of AES-NI
 - Likely the fastest CAESAR candidate on Intel Haswell processors
- Nonce-based

AEGIS: Properties

- Properties
 - Parallelizable: locally
 - No security reduction but easy to analyze
 - Not resistant to nonce reuse
 - Performance: size/speed tradeoff

AEGIS

- Design Rationale
 - Inspiration Pelican MAC
 - [Daemen-Rijmen'05]
 - 128-bit secret state
 - easy to analyze
 - secure up to birthday bound
 - 2.5 times faster than AES
 - Our design: Save the state after
 each AES round, then construct
 stream cipher from MAC



AEGIS

- Design Rationale (2)
 - Parallel AES round functions in each step so as to fill the AES instruction pipeline
 - AEGIS-128L can make full use of the 8-stage AES instruction pipeline of Haswell processor

AEGIS

- AEGIS-128L
 - 128-bit key, 1024-bit state
- AEGIS-128
 - 128-bit key, 640-bit state
- AEGIS-256
 - 128-bit key, 756-bit state
- Tag: 128-bit

AEGIS-128



AEGIS: Security Claims

- Requirements for secure implementation
 - each key and nonce pair can be used only once
 - if verification fails, the decrypted message and wrong message authentication tag should not be given as output
- Forgery attack: success prob. 2^{-t} with t the tag size
- Key and state cannot be recovered faster than brute force if forgery attack is not successful
 - 128-bit tags strongly recommended

AEGIS: Security Analysis

- Authentication
- Encryption
- Does authentication affect encryption?
 - short tag → easy forgery, and results in chosen ciphertext attack against encryption
- Does encryption weaken authentication?
 - ciphertext leaks state information, which may benefit a forgery attack
 - such as partial state value, state collision

AEGIS: Security

- Authentication
 - a difference in ciphertext passes through at least 4 AES rounds
 - stronger than Pelican MAC (4 AES rounds) since difference being distributed to at least 4 words
- Encryption
 - AEGIS encryption is a stream cipher with nonlinear state update function
 - differential and linear analysis is precluded

AEGIS: Security

Does authentication affect encryption?

- AEGIS without MAC is vulnerable to a chosen ciphertext attack
- To preclude chosen ciphertext attack
 - 1) if tag verification fails, the decrypted plaintext should not be given as output
 - the tag size should be sufficiently large to resist a chosen-ciphertext attack

(128-bit tag recommended)

AEGIS: Security

Does encryption weaken authentication?

- At each step, AEGIS leaks 128-bit keystream, i.e., 128bit state information
- The overall differential probability of the forgery attack against AEGIS increases
- But the differential probability that a difference propagates through 5 AES rounds is not affected
 - reason: at each step, the information leaked on $S_{i,j}$ is of the form:

$$S_{i,1} \oplus (S_{i,2} \& S_{i,3}) \oplus S_{i,4}$$

AEGIS: Security Randomness of keystream

- Recent results (Minaud, SAC 2014)
 - AEGIS-128
 - 2¹³⁰⁺ keystream bits for distinguishing
 - AEGIS-256
 - 2¹⁸⁰⁺ keystream bits for distinguishing
 - AEGIS-128L
 - So far, no results (expected to be strong)

Performance

- Speed on haswell processor (AEGIS-128L)
 - 0.30 cycles/byte (16KB messages)
 - 0.37 cycles/byte (4KB messages)
 - 0.51 cycles/byte (1KB messages)
 - 1.11 cycles/byte (256B messages)
 - 3.44 cycles/byte (64B messages)

Performance

titul)	vintermute	liydra9	Morinity	hydrað	Mity	hydrad	14459	146230	Modeat	hydrađ	hydra4	Matom	hydra7	Mandy	hydrai	
a gid ISI	acel 15 gen v1	angia) ISI	argid 11	argiellä	argiel I Si	argin) ISI	nena ViHivi	morus1250125v1	merus1250125v1	morus1250125V1	merus) 250125v1	morus\$60129/1	argin) ISI	morue\$6012\$V1	morue560128v1	noruski
tiaoniny1	acalifigen vi	tiaoniev'i	tiaetiev1	tiaexiev!	tiaoniev'i	tiaeriev1	menus) 256v1	morus1250256/1	morus1250256/1	morus1250256/1	meruel 280256v1	morus1250125v1	tiaedev'	morue1250125V1	morus1250125V1	noruel 13
angial II	neru6661v1	ang at 15	ușdii	argial 15	ang si 15	ang di S	nene Hivi	morus\$6012\$V1	morus\$60129v1	morue\$6012\$v1	morue640128v1	morue1250256/1	ang di S	morue1250256/1	moruel 250256/1	noruel 13
ergin255	nemi6661v1	11763	nter:	agilii	again -	argialii	17 Att	nem/6641v1	nerx\$661v1	ohaadity1ms3#1t125	vhaaditv1ms2ft1t125	nerx3261v1	argidiji	tertifii(1v1	ohaadity1ms3#1x256	sheederl
klanneg)25v1	nerr,3161v1	kiaaanagi 1994	kiaamegi 1991	elverv1	elverv1	diaeneg (1994	reviewi	halahlahl	halaviovi	ohaadiir/Imr3#11256	ohaadoto (mailte 16266	vheeditv1ms3ft1e125	elvervi	ten:32(1v)	ohaadevleeldelalls	sheedats'
send 1901 1971	nervádády)	elverv!	elvervi	kianneg 120v1	kiaaneg(19v1	elvervi	wheedowine:Mix125	oheedatvimeidritiis	okceátvimzifitizi	nemádálvi	nersééélvi	vheeditv1ms3ft1t256	morus1260129/1	nemšišivi	nemášší vi	uendele h
The second	morus60126v1	morus1250125v1	morus) 2501 2511	morus1260128/1	morue1260126v1	ility ility	vheedevlms3#1x256	oheeddovlmo3#1t256	nhaaditv1mr3#1t256	heldvlovi	heleviovi	nem/3261v1	kiananegi 1994	heleklev!	heldvlov1	helettert
elvervi	sendifi(v)	deexymeg128129v1	decopress (1911) Million (morus60128v1	merus60129v1	menut[180256/1	nhaadiin/Imr3fi34256	oheedatv1mr3#3x256	okceátvimzifiitis	vheedevlms3634256	vhaaditv1ms3#34256	vheeditv1ms3ft3t256	morus660129v1	acel 13 gen vl	ohaadity1ms3834256	sheederi
morus\$(0129/1	110007011	Annual 25612971	decoy mag 26123v1	merus1200256/1		deexy meg 125125v1	nen3161v1	ner:3341v1	tiaoninv1	nem21211v1	nen:3161v1	nervéčélvi	morus1280256/1	tiaetiev!	halawi	uldwl
kianagi 151vi	aacon 125v1	Kanagilawa	and the second sec	according (Million)	deexymegi2\$12\$v1	deany mag256128v1	namálólóv".	nemáčšáv!	nersékév!	tiaender/1	tiaerdev1	tiaeniev!	deaxy mag 128128v1	ohaaddovlme3ff1t125	amon96/1	ucon90/1
ácoxymeg128126v1	acel 25otrevil	morus1250256/1	meruri 200256/1	deexymeg256128v1	deexymeg256125v1	morus60125v1	halaiwi	haldwl	nerx3241v1	nersátáár)	nersőddév)	hal diviev)	deexy meg 256128v1	ohaaditv1mr3fr1t256	nemádálvi	sendili h
ácoxymeg256128v1	acel 15otryvl	itony mg 120120v1	Story and Hilling	kianagi 1971	kianagi 1971	kianag 120vi	ugólii	argin) III	bilitivil	heldwi	halaiw)	amon96/1	danagi 1941	ugidili	nen:500ml	uandilik
acel 28 gen vl	acel/Sotrey1	morus\$(0129/1	merus60128v1	acel Diopfor 1	acellicyfivi	deany ang 12512511	namátály!	neruščiši vi	argiellSi	nemádálv1	nerušćši v l	argialisi	acel 15 cpfby 1	acdifigenvi	nend261v1	uen 336 h
acel36gemv1	acejambor 1	deexymeg256128v1	deceny mag 256128v1	acel 15 gen vl	acelligenvi	daany 10 g256128v1	aacon96/1	ascon90/1	nerušćšivi	secon96v1	1000096V1	nemálólóvi	aced 15 genwi	helew!	angin) ISI	agid Bi
ácoxymog 128126v1	acalificity/1	acelligenvi	acel 25 gem vl	deexyseg125125V1	deexyseg125125v1	acelligenvi	ace al M	angial 25	ascen90/1	artici III	artic) ISI	vheeditv1mr587h256	acd36gemv1	ohaadite/Imr060x256	ang di S	aga B
acel Diogenvi	om deta 5126512x250x1	acaliticyfiwl	acel 15 cptby 1	acilfógenvi	acultógenvi	acellifeyfovl	nem3161v1	ner:3261v1	acgial25	acgidill	ugid 25	nemušišivi	dearly and 120120v1	nem 3261v1	ohaadity1ms587k256	sheedayl
ásonymeg256128v1	om deta 512k256x256x256x1	acalifigenvi	acc266gemv1	6coxyscg256129v1	deenyeeg256125v1	acd36gemv1	vhaadiiv(ms5674256	nheedatv1mr587x256	nhaaditv1mr587k256	nem3161v1	norr.3161v1	actici II	daan yaa gii dala ili biyi	uşdili	secon129v1	ud divitivi
nervádálvi	emőékaőlőkiőőniőBtaulóBvi	acalificgebyl	accittlepter)	neru6661v1	neru6661v1	acd36cpfbv1	angia Si	101011	nerx3261v1	vhaadevlms567x256	vhaaditv1ms5871256	halaiwi	neműélél vi	ner:////	ang ka Si	accentility
acelificpfiv)	eribob192r1	neroséél vi	send&divi	actificpfor1	actificper/	nerośćći vi	accon125v1	ascen125v1	halavhivi	helevkivi	helevhivl	asten 129/1	acalificpfor)	agidSi 👘 👘	piédeipher 126v1	apidi
nervédőlv1	omádia 156k 115k 96ta ušév 1	heletter!	helevievi	nerv3161v1	nerv3161v1	nend161v1	elvervl	elverv1	ning	ugidSi 👘	upi04	1070255	nen 1141vi	helevhivi	riédzinher256v1	(Keiphe
halaivievi	om deta 156k 119n 96ta 1997 1	oheedatvimei#itiii	oheedevlersteltste	haldvlovi	haldvlovi	nemádálv1	pi66cipher128v1	acel28gemv1	ascen129v1	secon129v1	agen129v1	acel 26gem vl	nemű461v1	kiannegi 20vi	elvervi	(Keiphe
nem 2041 v1	om deha 256k 192n 100tau 125v 1	nheedatv1mr3#1x256	oheedevlorideltill	nemi6661v1	nemi6661v1	ohaadev1ms261t125	piéécipher256v1	pi64cipher128v1	elverv!	elverv1	elverv1	halahhiri	heldvlovi	ercam10/2	ner:3261v1	then
vheeditv1mr3ft1t125	om deta 256k 128x 96ta a 128v 1	ners2261v1	sen 21/21v1	wheedetv1ms2#1x256	oheedetvims261t125	ohaadity1ms1#1x256	(cepele)2fav)	piólaiphar256v1	acel 28gemvl	piéleigher256v1	piédaiphan256v1	kianneg(1394)	ohaaditvims201t256	ercam10v1	icepole 128av1	uen 2161 v
vheeditv1mr3#1r256	om deta 256k 256n 100ta u 160v 1	nemskál vi	senskálvi	vheedevims201t125	nheedetvimsitrititis	heldvlovi	icepole196av1	icepole128av1	ri 64a iphari 120vi	tiéleigher120v1	siddelpher 120v1	riðicipker250/1	ohaaddovlime3dtile128	142 on 96/1	copolo256av1	tepidi
niewi	om déa 1966 1966 188 au 1967 1	ohaadar/Ims2020255	oheeder/Ims2626256	Material	halawi	ohaadity/ims2020256	icegole (1994)	copole266av1	(Maigher2601	teepole256av1	leepole 266v)	pi 64ei pheri 120vi	lelewi	eream 12v2	cepsie 120v1	tepieli
nerskiller!	akekeyakv!	alew!	histori	whee detv1ms2#24256	ohaadder Inns Miller 196	lalaw!	aeri Meyter)	copole (1204)	cepele 128av1	teepole12fav1	icepole (18av)	acultógenvi	ohaaddoolma2#2x256	oheedavimetti 1256	(Deipher256r)	tepiel)

- Likely the fastest on Haswell
- Quite fast on platforms with no AES-NI

Conclusions

- Simple design
- Likely the fastest on Haswell processors
 - Targeting platforms with AES-NI
 - Also fast for short messages
- Strong in security