WILL THE FUTURE LIGHTWEIGHT STANDARD BE RISC-V FRIENDLY?

Gorkem Nisanci[1,4], Remzi Atay[2], Meltem Kurt Pehlivanoglu[2,3],
Elif Bilge Kavun[3] and Tolga Yalcin[4]

1. Eastern Mediterranean University, Famagusta, Cyprus
2. Kocaeli University, Kocaeli, Turkey
3. University of Sheffield, Sheffield, United Kingdom
4. Northern Arizona University, Flagstaff, Arizona

Overview

- Why RISC-V
- NIST LWC Competition 2nd Round Finalists
- Evaluation Strategy
- Windows Results
- Linux Results
- Windows vs. Linux
- Future Work
- Remarks and Comments

WHY RISC-V?

Open Source – Open Instruction Set

- NO licensing!
- NO royalties!
- NO lawyers!
- ALLOWS proprietary implementations
- FUTURE standard for all computing devices – microcontrollers to supercomputers (a little too ambitious!?)
- STRONG support from both academia and industry (well, most of it anyways!)

Why RISC-V?

NIST Lightweight Cryptography Competition

- Little published work on cryptography on RISC-V!
- Is RISC-V suitable for cryptography – specifically lightweight cryptography?
- RISC-V flavors:
  - **R32I: Base Integer Instruction Set, 32-bit (FROZEN)**
  - **R32E: Base Integer Instruction Set (embedded), 32-bit, 16 registers (OPEN)**
  - **R64I: Base Integer Instruction Set, 64-bit (FROZEN)**
  - **R128I: Base Integer Instruction Set , 128-bit (OPEN)**
- Our choice: **R32I**
  - **Extensive documentation**
  - **Stable (!) development tools on both Windows and Unix**

NIST LWC Competition Second Round Finalists

32 Second Round Finalists

- 18 of them with permutation based construction
  - **ACE, Ascon, DryGASCON, Gimli, ISAP, KNOT, ORANGE, Oribatida, PHOTON-Beetle, SAEAES, SPARKLE, SPIX, SpoC, Spook, Subterranean, TinyJAMBU, WAGE, Xoodyak**
- 13 of them with block cipher mode of operation based construction
  - **COMET, Elephant, ESTATE, ForkAE, GIFT-COFB , HyENA, LOTUS-LOCUS, mixFeed, Pyjamask, Romulus, Saturnin, SKINNY, SUNDAE-GIFT**
- 1 of them with stream cipher mode of operation based construction
  - **Grain-128AEAD**

Evaluation Strategy

Evaluation both on Windows and Linux

- Windows based evaluation using OVP tools based on gcc-4.9.1 running on Windows 10
- Linux based evaluation using RISC-V GNU toolchain based on gcc-9.2.0 running on Lubuntu Eoan Ermine 19.10
- C codes provided on NIST LWC Competition site used – no optimizations
- Only recommended parameter sets evaluated
- Each code compiled with different optimization options:
  - **O0, O1, O2, O3, Ofast, Os**
- Each algorithm evaluation in authenticated encryption/decryption mode with 3 different packet sizes:
  - **128 bytes, 2 KB, 16 KB**

EVALUATION STRATEGY

Size Evaluation

- For each code:

  `$ rv-gcc -c -o O0.o main.c -DRISCV32 -O0/O1/O2/O3/Ofast/Os -g`

  executed – with all optimization options
- Followed by:

  `$ rv-nm -t d -S --size-sort *.o`
- Windows: **`rv-gcc`** and **`rv-nm`** aliased to **`riscv-none-embed-gcc.exe`** and **`riscv-none-embed-nm.exe`**, respectively
- Linux: **`rv-gcc`** and **`rv-nm`** aliased to **`riscv64-unknown-elf-gcc`** and **`riscv64-unknown-elf-nm`**, respectively

Evaluation Strategy

Speed Evaluation

- For each algorithm, four `main` functions defined:
  - **main1.c: Parameter initialization only**
  - **main2.c: Parameter and packet initialization**
  - **main3.c: Parameter/packet initialization and encryption**
  - **main4.c: Parameter/packet initialization, encryption and decryption**
- Execution times for encryption and decryption calculated by subtracting initialization times from overall computation times – both in terms of cycles
- Windows execution times using ISS (Imperas Instruction Set Simulator)
- Linux execution times using Spike (RISC-V ISA simulator)

Windows Results – Size

Code Size (bytes)

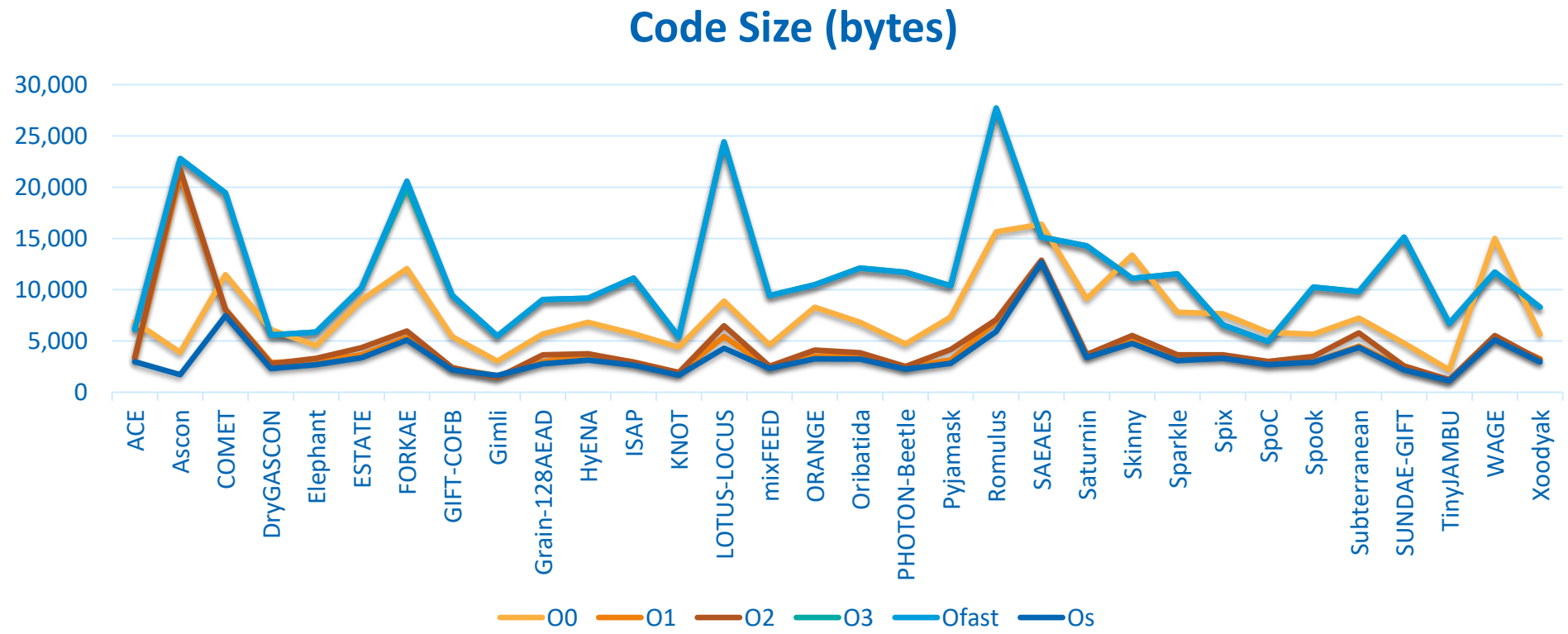
Algorithm	O0	O1	O2	O3	Ofast	Os
ACE	6,876	3,202	3,374	6,134	6,134	2,976
Ascon	3,890	21,222	21,716	22,784	22,784	1,718
COMET	11,464	8,098	8,056	19,444	19,444	7,482
DryGASCON	6,102	2,920	2,772	5,578	5,578	2,322
Elephant	4,562	3,064	3,310	5,874	5,874	2,696
ESTATE	8,986	3,648	4,350	10,180	10,180	3,378
ForkAE	12,075	5,349	5,979	20,065	20,595	5,111
GIFT-COFB	5,434	2,362	2,406	9,464	9,464	2,186
Gimli	3,040	1,610	1,444	5,474	5,474	1,638
Grain-128AEAD	5,687	2,973	3,653	9,033	9,033	2,779
HyENA	6,828	3,684	3,752	9,174	9,174	3,144
ISAP	5,706	2,964	2,936	11,142	11,142	2,660
KNOT	4,397	1,923	1,935	5,417	5,417	1,675
LOTUS-LOCUS	8,886	5,444	6,480	24,408	24,408	4,300
mixFeed	4,615	2,431	2,557	9,443	9,443	2,349
ORANGE	8,296	3,520	4,126	10,478	10,478	3,268

Windows Results – Size

Code Size (bytes)

Algorithm	O0	O1	O2	O3	Ofast	Os
Oribatida	6,824	3,606	3,856	12,116	12,116	3,236
PHOTON-Beetle	4,704	2,426	2,524	11,704	11,704	2,262
Pyjamask	7,342	3,166	4,182	10,374	10,374	2,820
Romulus	15,650	6,896	7,094	27,716	27,716	5,924
SAEAES	16,404	12,832	12,884	15,120	15,120	12,684
Saturnin	9,124	3,512	3,688	14,292	14,292	3,390
SKINNY	13,384	5,268	5,542	11,114	11,114	4,764
SPARKLE	7,808	3,606	3,654	11,534	11,534	3,096
SPIX	7,662	3,544	3,644	6,580	6,580	3,320
SpoC	5,836	2,800	3,002	4,954	4,954	2,700
Spook	5,664	2,944	3,504	10,262	10,262	2,924
Subterranean	7,246	4,504	5,808	9,814	9,814	4,366
SUNDAE-GIFT	4,782	2,302	2,570	15,140	15,140	2,182
TinyJAMBU	2,196	1,204	1,228	6,726	6,726	1,136
WAGE	15,002	5,258	5,538	11,718	11,718	5,116
Xoodyak	5,629	3,275	3,175	8,299	8,299	2,955

Windows Results – Size



Windows Results – Speed

Execution Time (cycles/byte) – fastest (–O3 option)

Algorithm	128 Byte packets		2 KB packets		16 KB packets	
	ENC	DEC	ENC	DEC	ENC	DEC
ACE	7531.13	7533.27	4986.99	4989.46	4838.58	4841.07
Ascon	160.56	157.78	113.28	114.39	110.52	111.86
COMET	173.84	172.19	127.82	125.04	125.11	122.25
DryGASCON	922.59	922.79	727.8	727.75	716.44	716.38
Elephant	124088.51	124088.52	95344.61	95344.61	93690.62	93690.61
ESTATE	383.97	384.2	338.41	338.42	331.64	331.65
ForkAE	3496.27	5925.12	3248.6	5677.62	3234.15	5663.19
GIFT-COFB	1499.19	1499.15	1218.99	1219.11	1202.65	1202.77
Gimli	694.87	699.59	477.67	481.71	465	469
Grain-128AEAD	32363.42	32272.98	26578.84	26491.22	26239.49	26151.97
HyENA	10882.96	10888.13	8753.61	8759.79	8629.4	8635.64
ISAP	3238.33	3238.83	1418.04	1418.07	1382.38	1382.38
KNOT	263.65	263.34	196.48	196.46	192.56	192.56
LOTUS-LOCUS	20167.54	20167.52	18064.06	18064.05	17941.36	17941.36
mixFeed	829.66	829.34	531.74	531.54	514.36	514.17
ORANGE	9028.99	9029.1	6206.87	6207.05	6041.74	6041.93

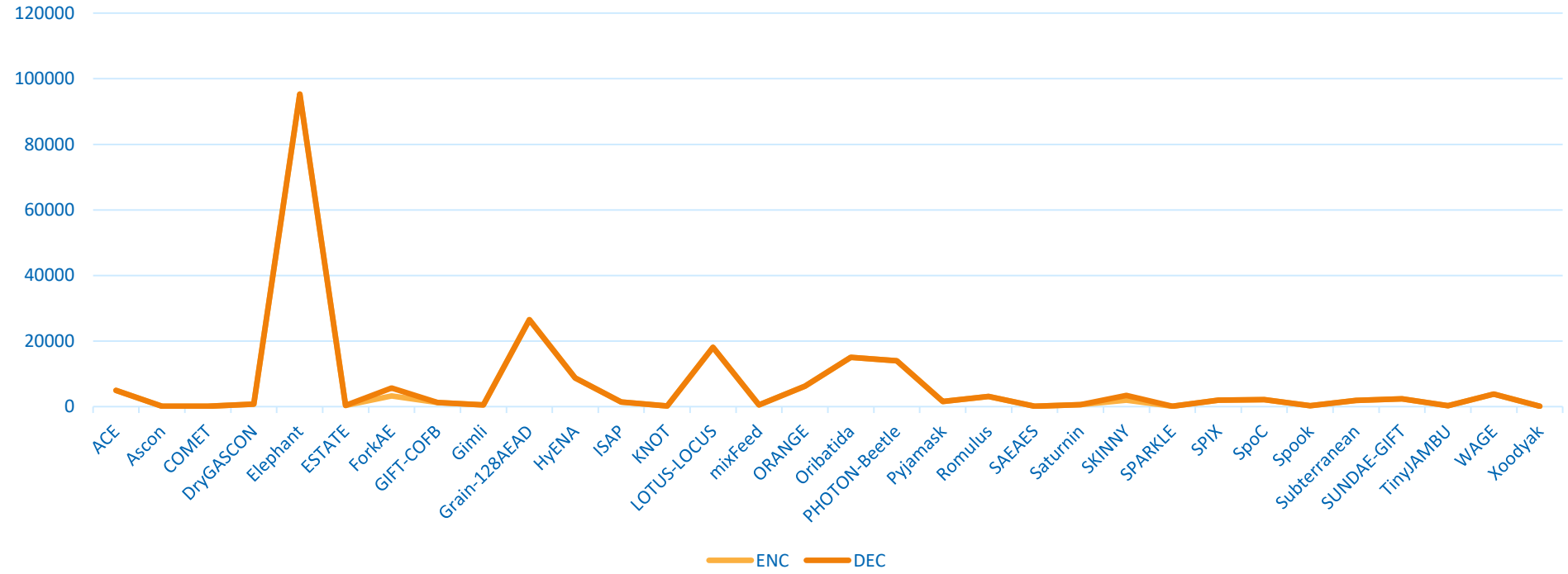
Windows Results – Speed

Execution Time (cycles/byte) – fastest (–O3 option)

Algorithm	128 Byte packets		2 KB packets		16 KB packets	
	ENC	DEC	ENC	DEC	ENC	DEC
Oribatida	18544.84	18535.95	15067.36	15058.19	14864.51	14855.31
PHOTON-Beetle	17203.41	17205.45	13988.74	13988.83	13797.36	13797.33
Pyjamask	2421.3	2423.02	1551.69	1553.5	1500.97	1502.78
Romulus	3413.72	3414.39	3057.21	3057.72	3036.43	3036.93
SAEAES	155.66	155.59	128.68	128.67	127.1	127.1
Saturnin	893.09	894.27	612.23	612.3	595.84	595.85
SKINNY	2459.7	3909.59	1997.15	3446.73	1970.18	3419.75
SPARKLE	212.34	213.22	121.52	123.33	116.13	118.03
SPIX	3417.53	3419.64	1992.86	1995.33	1909.75	1912.24
SpoC	2538.1	2536.77	2159.26	2158.24	2137.16	2136.15
Spook	517.85	515.54	310.16	304.68	298.05	292.38
Subterranean	3504.52	3505.66	1922.47	1923.01	1830.19	1830.69
SUNDAE-GIFT	2819.77	2820.14	2397.7	2397.78	2373.08	2373.14
TinyJAMBU	263.46	263.26	236.08	236.06	234.48	234.48
WAGE	5738.55	5738.35	3823.66	3823.88	3711.96	3712.2
Xoodyak	191.48	189.23	118.92	116.55	114.64	112.26

WINDOWS RESULTS – SPEED

Execution Time (cycles/byte) – fastest (–O3 option)



Linux Results – Size

Code Size (bytes)

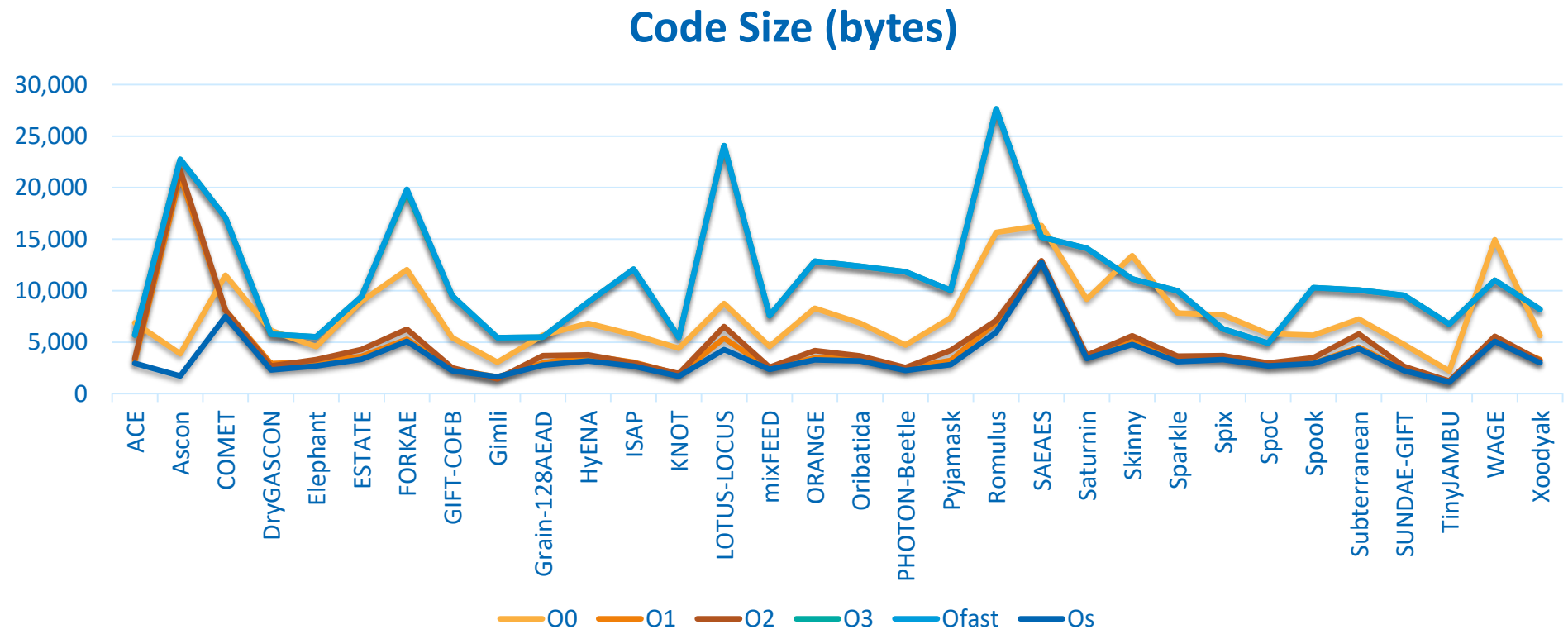
Algorithm	O0	O1	O2	O3	Ofast	Os
ACE	6,864	3,154	3,392	5,704	5,704	2,946
Ascon	3,868	21,128	21,690	22,756	22,756	1,706
COMET	11,502	8,092	8,088	17,088	17,088	7,494
DryGASCON	6,122	2,918	2,698	5,772	5,772	2,296
Elephant	4,566	3,070	3,308	5,506	5,506	2,702
ESTATE	8,968	3,622	4,292	9,414	9,414	3,344
ForkAE	12,041	5,271	6,257	19,633	19,843	5,085
GIFT-COFB	5,446	2,384	2,498	9,490	9,490	2,240
Gimli	3,042	1,610	1,424	5,446	5,446	1,642
Grain-128AEAD	5,681	2,967	3,697	5,481	5,481	2,779
HyENA	6,836	3,686	3,758	8,876	8,876	3,184
ISAP	5,728	3,038	2,964	12,098	12,098	2,674
KNOT	4,401	1,883	1,943	5,467	5,467	1,685
LOTUS-LOCUS	8,748	5,386	6,526	24,092	24,092	4,270
mixFeed	4,593	2,453	2,563	7,565	7,565	2,363
ORANGE	8,298	3,456	4,168	12,854	12,854	3,290

Linux Results – Size

Code Size (bytes)

Algorithm	O0	O1	O2	O3	Ofast	Os
Oribatida	6,838	3,588	3,672	12,372	12,372	3,190
PHOTON-Beetle	4,718	2,428	2,532	11,834	11,834	2,248
Pyjamask	7,352	3,238	4,204	10,024	10,024	2,828
Romulus	15,668	6,920	7,114	27,652	27,652	5,942
SAEAES	16,322	12,818	12,902	15,190	15,190	12,742
Saturnin	9,148	3,510	3,704	14,108	14,108	3,396
SKINNY	13,392	5,274	5,610	11,126	11,126	4,782
SPARKLE	7,822	3,584	3,638	9,986	9,986	3,110
SPIX	7,646	3,492	3,696	6,296	6,296	3,296
SpoC	5,828	2,750	2,978	4,892	4,892	2,688
Spook	5,680	2,958	3,494	10,286	10,286	2,920
Subterranean	7,244	4,520	5,784	10,062	10,062	4,364
SUNDAE-GIFT	4,782	2,308	2,648	9,548	9,548	2,234
TinyJAMBU	2,200	1,214	1,234	6,754	6,754	1,128
WAGE	14,944	5,212	5,568	11,002	11,002	5,078
Xoodyak	5,643	3,311	3,197	8,193	8,193	2,985

Linux Results – Size



Linux Results – Speed

Execution Time (cycles/byte) – fastest (–O3 option)

Algorithm	128 Byte packets		2 KB packets		16 KB packets	
	ENC	DEC	ENC	DEC	ENC	DEC
ACE	7990.81	7240.16	4841.92	4796.01	4658.68	4652.94
Ascon	817.80	192.62	100.91	61.90	59.29	53.96
COMET	1060.52	190.02	196.87	141.91	147.22	137.97
DryGASCON	1446.23	780.53	663.04	622.21	617.67	612.62
Elephant	27650.02	26983.90	20777.96	20737.21	201.55	40558.21
ESTATE	1212.52	467.91	460.79	415.12	458.85	442.20
ForkAE	4328.18	5990.49	3376.48	5663.49	3320.92	5644.85
GIFT-COFB	4619.23	3874.38	3195.89	3149.45	3113.19	3107.60
Gimli	1370.56	742.80	537.37	494.76	486.79	482.23
Grain-128AEAD	33504.79	32682.17	26954.88	26808.93	26574.20	26466.56
HyENA	10474.95	9788.48	7872.83	7840.43	7721.47	7726.34
ISAP	3675.79	3010.60	1151.08	1110.34	1009.71	1004.51
KNOT	855.14	191.24	175.80	139.25	137.90	134.58
LOTUS-LOCUS	19890.22	19026.15	17099.79	17044.40	16937.44	16928.34
mixFeed	1552.04	888.38	610.34	570.13	555.24	551.71
ORANGE	10003.92	9219.23	6386.48	6338.37	6175.29	6169.44

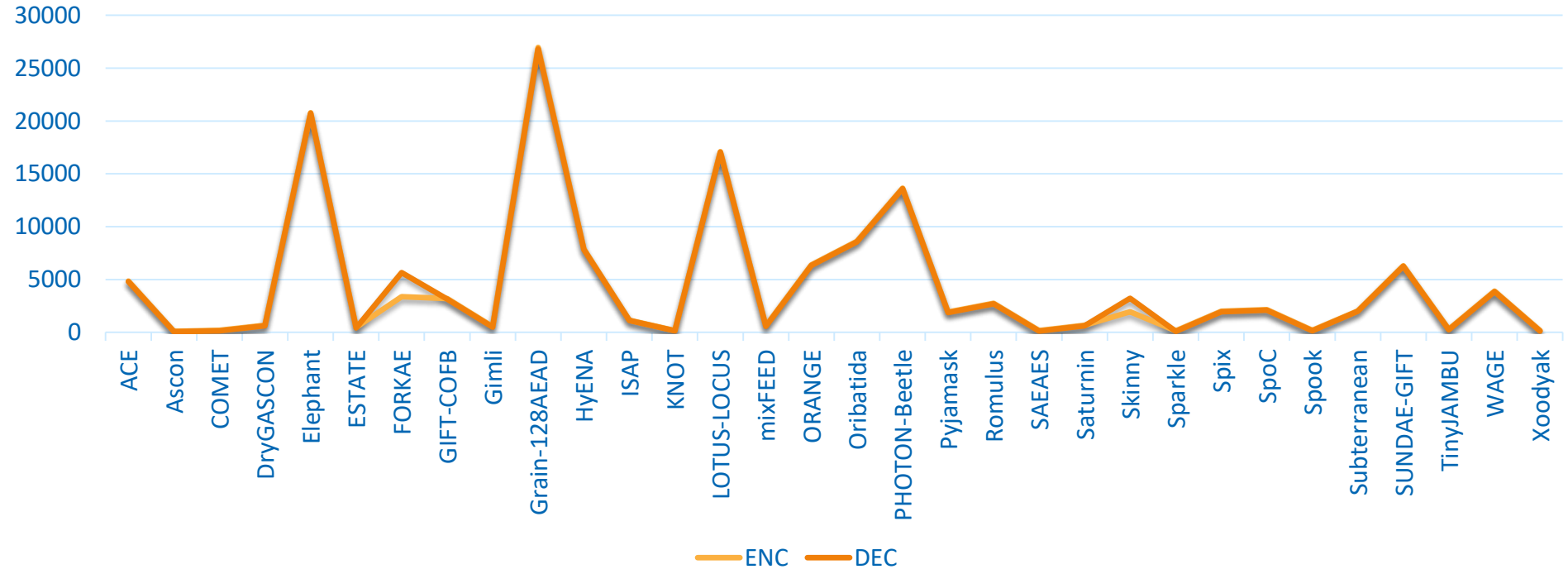
Linux Results – Speed

Execution Time (cycles/byte) – fastest (–O3 option)

Algorithm	128 Byte packets		2 KB packets		16 KB packets	
	ENC	DEC	ENC	DEC	ENC	DEC
Oribatida	11362.81	10520.34	8600.56	8546.55	8422.18	8422.85
PHOTON-Beetle	17453.46	16717.35	13632.23	13591.71	13425.82	13366.70
Pyjamask	3666.72	2933.59	1918.60	1871.54	1817.19	1808.88
Romulus	3783.66	3014.01	2738.74	2700.27	2678.24	2681.52
SAEAES	981.39	155.25	181.22	129.53	134.87	127.64
Saturnin	1622.70	927.92	672.49	628.31	616.74	611.03
SKINNY	3126.25	3672.16	1950.57	3233.14	1882.44	3207.04
SPARKLE	857.59	217.43	138.81	96.27	96.35	90.41
SPIX	4053.91	3343.12	1996.06	1952.52	1876.46	1870.91
SpoC	3155.99	2381.16	2136.99	2086.70	2077.06	2070.77
Spook	993.06	250.78	198.42	152.84	152.39	146.75
Subterranean	4369.31	3625.39	2031.60	1986.45	1895.67	1890.35
SUNDAE-GIFT	8071.36	7350.55	6292.70	6246.77	6163.51	6225.59
TinyJAMBU	921.18	271.46	286.04	244.53	248.49	243.42
WAGE	6529.60	5777.48	3903.92	3856.85	3751.19	3754.21
Xoodyak	932.54	177.01	158.14	110.28	113.34	105.87

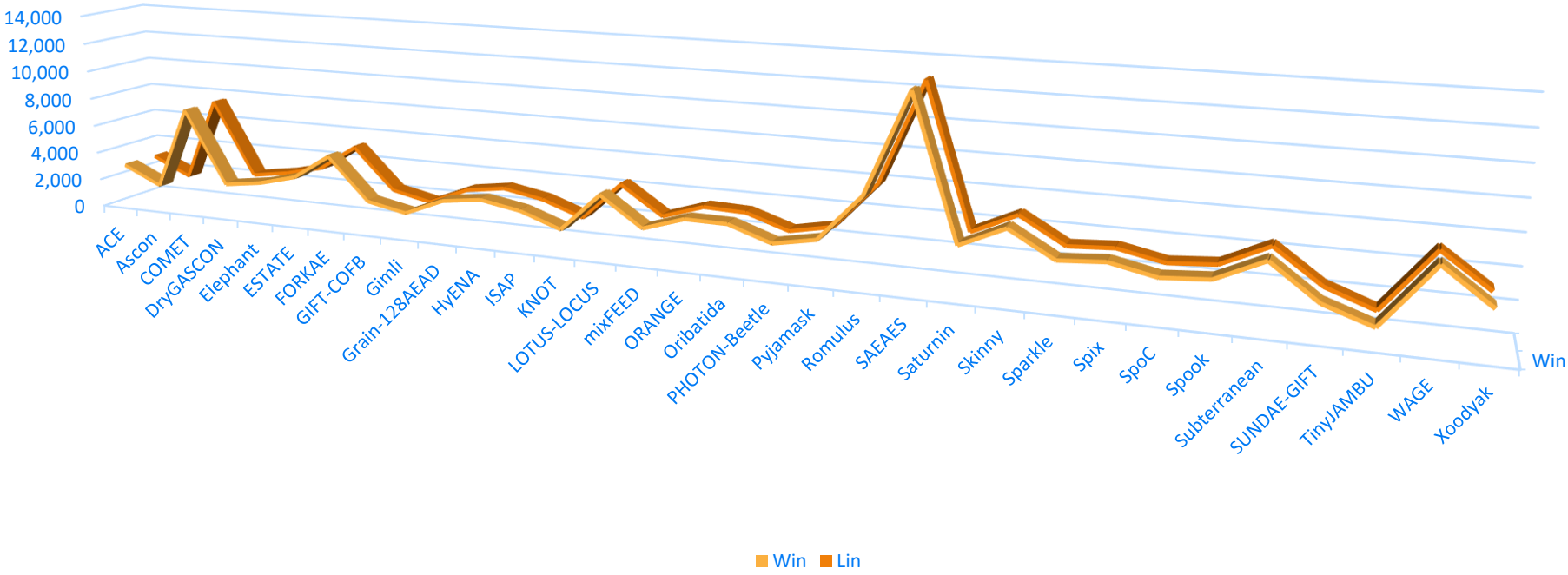
Linux Results – Speed

Execution Time (cycles/byte) – fastest (–O3 option)



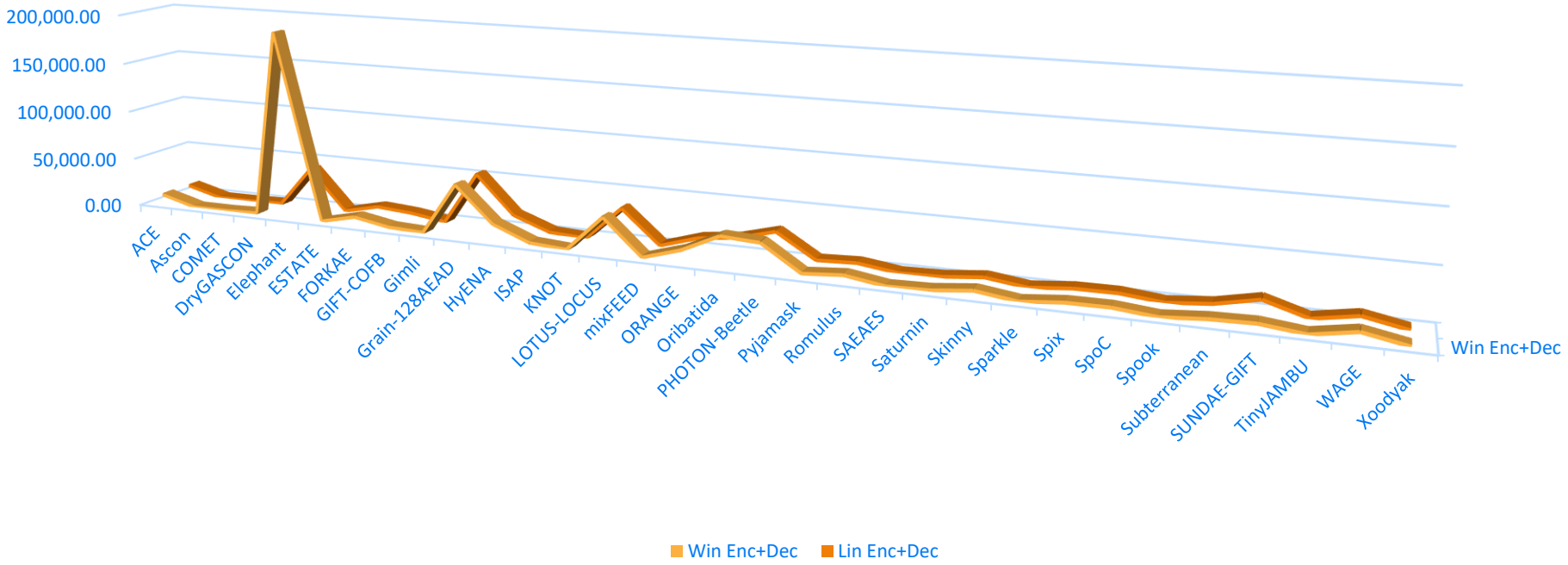
WINDOWS VS LINUX – SIZE

Code Size (bytes) – Os option



Windows vs Linux – Speed

Execution Time (cycles/byte) – fastest (–O3 option)



Future Work

Code Optimization

- Investigation of codes in Assembler
- Optimization of low-level functions
- “Lightweight cryptography” specific instruction and supporting co-processor development
- All three action items already in progress
- Results confidential :(
- We will share as much as we can :/
- Happy to share the current results in detail (see the example →)

ACE Functions/Consts	O0	O1	O2	O3	Ofast	Os
rate_bytes	8	8	8	8	8	8
RC0	16	16	16	16	16	16
RC1	16	16	16	16	16	16
RC2	16	16	16	16	16	16
SC0	16	16	16	16	16	16
SC1	16	16	16	16	16	16
SC2	16	16	16	16	16	16
ace_permutation_ALLONE	82	36	26	32	32	30
ace_permutation_ALLZERO	92	52	50	92	92	54
ace_print_state	98	64	62	62	62	72
ace_print_data	104	74	82	82	82	76
rotl8	114	20	20	20	20	20
ace_gentag	444	192	200	506	506	192
ace_ad	614	288	294	430	430	256
ace_init	632	258	258	778	778	268
crypto_aead_encrypt	1034	512	484	714	714	448
crypto_aead_decrypt	1054	558	498	1220	1220	464
ace_permutation	1216	660	776	1590	1590	600
simeck64_box	1288	384	520	504	504	392
SUM	**6876**	**3202**	**3374**	**6134**	**6134**	**2976**

Remarks and Comments

- SPECK-128/128 (fastest software cipher) evaluated to provide reference:

SPECK 128/128	ENC	DEC	
Execution time (cycles/byte)	139		Atmel ATmega128 high-tput
	451.81	**495.88**	**RISC-V R32I -O3 option**
Code size (bytes)	214		Atmel ATmega128 low-flash
	716		**RISC-V R32I -Os option**

- Although not a fair comparison, at least provides a scaling factor estimate for ASM vs C implementation
- It is possible to improve both code size and execution time via custom instructions with minimal area overhead
- Greatest challenge: Toolchain – setup complicated, output not yet optimal, needs to be improved

Remarks and Comments

Thanks for listening!

QUESTIONS?