# High-speed high-security cryptography on ARMs

Daniel J. Bernstein

Research Professor, University of Illinois at Chicago Professor, Cryptographic Implementations, Technische Universiteit Eindhoven

Tanja Lange

Professor, Coding and Cryptology, Technische Universiteit Eindhoven

joint work with: Peter Schwabe, Academia Sinica

"Don't roll your own crypto. Leave it to us."

# Speed of cryptography: http://bench.cr.yp.to

• •			Introduction - 0	hromium			- 0
() Introduction ×							
← → C (③ bench.cr.yp.to)							公 <b>4</b>
eBA vice definition and reparameter labor vice definition and reparameter labor vice definition and vice def	CS: ECR	YPT Be	nchmarkin	g of Cryptogr	aphic Syst	ems	<b>ECRYPT II</b> ⊥াদ-তারু্টা^ ‡
General information:	Introduction	eB.	ASH eBAS	C eBATS	SUPERCOP	XBX	Computers
How to submit new software:	Hash fu	nctions	Stream ciphers	DH functions	Public-key	encryption	Public-key signatures
List of primitives measured:	SHA-3 finalists	All hash function:	s Stream ciphers	DH functions	Public-key	7 encryption	Public-key signatures
Measurements indexed by machine:	SHA-3 finalists	All hash function:	s Stream ciphers	DH functions	Public-key	encryption	Public-key signatures
Users of cryptography have a choice of pu PowerPC, etc.? How much network band sharing, secret-key encryption, and hash fi	width do the system: inctions.	s consume? The sa	me questions arise for ma	ny other cryptographic operati			
eBACS (ECRYPT Benchmarking of Cry	ptographic Systems)	aims to answer the	ese questions. eBACS un	fies and integrates			
eBATS (ECRYPT Benchmarking     eBASC (ECRYPT Benchmarking     eBASH (ECRYPT Benchmarking	of Stream Ciphers),	a continuation of th	e benchmarking carried (	out in eSTREAM, the ECRYPT	f Stream Cipher Projec	t; and	
The eBACS/eBATS/eBASC/eBASH ma	ling list is named afte	r eBATS, the first	of these projects. To join	the mailing list, send an empty	message to ebats-sub	oscribe at lis	t.cr.yp.to.
eBACS is organized by ECRYPT II, a N ECRYPT's 'Virtual Application and Impler within the European Commission's Sixth F United States National Institute of Standar	nentation Research L ramework Programm	ab (VAMPIRE). I ne (FP6), contract	ECRYPT II began 1 Aug number IST-2002-5079	ust 2008. Some components of 32. Many further improvements	f eBACS began earlier, to eBACS have been	as part of ECR funded by grant	YPT, a Network of Excellence
If you use eBACS information in a paper t	hen you should cite t	he web pages as fo	ollows:				

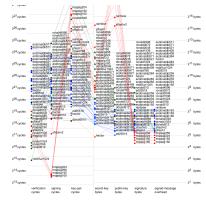
# Speed comparison of the SHA-3 finalists

crypto_sha3 skein512512 blake512 sha512 keccakct024r Long messages skein512256 blake512 sha552 rroset1	bund3jh52*groest1512 http://bench.cr.yp.tc 2012112: 55 round3jh256
amd64 IB+AES	Marcy, 3 x (3000Marc) (913) total (200 x 3000Marc) (913) total (200 x 3000Marc) (913) total (200 x 3000Marc) (9100Marc) (910Marc) (9100Marc) (9100Marc) (9100Marc) (9
amd64 SB+AES	byteck +1 2009042 2021 MM 2004 ED 1223, average 1420 (2014) (property R023 magnet: a 1 2006045; 2021 MM 2004 (2014) (property R023 magnet: a 1 2006045; 2021 MM 2014 (2014) (property R023 mitter, 4 1 200905; 2021 MM 2014 (2014) (2014) (2014) (property R023 mitter, 4 1 200905; 2021 MM 2014 (2014) (2014) (2014) (property R023 mitter, 4 1 200905; 2021 MM 2014 (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014) (2014
amd64 Sandy Bridge	Minualy, 2 a 1200MH4, 2011 1004 Care & 2220M, sim044, Sanda Bintige (20147); separate-SCIII
	torage 2 x 5660465 3111 triat Carn in 20100, anditi, Eanty Reign (20147), neproceeding
amd64 Westmere+AES	3ydex, 4 x 3430M92, 2023 Mill 2004, 2013 Mill 2004, 2013 Mill 2004, 2013 Mill 2004, 2013 Mill 2004, 2014 Mill 2004, 2014
amd64 Nehalem 🚺 🏌 📜 🧎 🚺	Raugue, B x 20008888; 2008 http://doi.org/10.0008/j.auguesspirities/ rturclus, 4 x 20008882; 2008 http://doi.org/10.0004/j.auguesspirities/ rturclus, 4 x 2000882; 2008 http://doi.org/10.0004/j.auguesspirities/ rturclus, 4 x 20008882; 2008 http://doi.org/10.0004/j.auguesspirities/ rturclus, 4 x 20008882; 2008 http://doi.org/10.0004/j.auguesspirities/ rturclus, 4 x 2000882; 2008 http://doi.org/10.000482; 2008 http://doi.org/10.000484; 2008 http://doi.org/10.000484; 2008 http://doi.org/10.000484; 2008 http://doi.org/10.000484; 2008 http://doi.org/10.000484; 2008 http://doi.org/10.00048; 2008 http://doi.org/
imd64 C2 45nm	
amd64 C2 65nm	
amd64 K10 32nm	hpind. 4 x 200046; 2011 AMD AN 2005, amothe A22 ADM - 100707-0108 hpind: 4 x 200046; 2011 AMD AN-2005, amothe A23 ADM - 100707-0108 hpind: 4 x 200046; 2011 AMD AN-2005, amothe A23 ADM - 100707-0108
amd64 K10 45nm	Jacks 1 + 200004, 2011 MD Plants 1 - 0 (1207) register         Fill MD Plants 1 - 0 (1207) register         Fill MD Plants 1 - 0 (1207) register           March 1 - 200004, 2011 MD Plants 1 - 0 (1207) register         Fill MD Plants 1 - 0 (1207) register         Fill MD Plants 1 - 0 (1207) register           March 1 - 200004, 2011 MD Plants 1 - 0 (1207) register         Fill MD Plants 1 - 0 (1207) register         Fill MD Plants 1 - 0 (1207) register           March 1 - 200004, 2014 MD Plants 1 - 0 (1207) register         Fill MD Plants 1 - 0 (1207) register         Fill MD Plants 1 - 0 (1207) register           March 1 - 200004, 2014 MD Plants 1 - 0 (1207) register         Fill MD Plants 1 - 0 (1207) register         Fill MD Plants 1 - 0 (1207) register           March 1 - 200004, 2014 MD Plants 1 - 0 (1207) register         Fill MD Plants 1 - 0 (1207) register         Fill MD Plants 1 - 0 (1207) register
amd64 K10 65nm	rauger 4 x 2008/Mid, 2008 AMD Presses Bibl, innelit, K14 Hove (13972); speroprikAM
amd64 K8	ana 2 x 2000/06/2 2000 AMD 2000m 64 XX, area(6,100 m)
· · · · · · · · · · · · · · · · · · ·	prist, 4 x 2008/04/, 2006 AADD Cybrew 2023, aweidd, 92 (19733); esperage-965
amd64 Piledriver	www.serg. 2 x 2006.042, 2012 AND A 13-A0304, WINEL, PORTAR (1619), approx. speak, 2 x 2000.042, 2012 AND A13-000000, amount, PORTAR (1619), approx.
amd64 Bulldozer	λρουά 4 × 130090, 2021 AMD 7 4-2126, weeks, Bohainer (M072), equerary-EGG           κατακαία + ν κλιθιάται (κατά τη διατη δι
amd64 Bobcat	Matter 2 + 1605647 (2014 AUX C), and a set of the set o
amd64 Nano 🛛 🙀 📢 🦂 🖌	Minus, 3 x 2020946; 2020 Vie Kawa (2020); awaidi, Nawa (202); awaidi, Nawaidi, Nawa (2
amd64 Atom	Mattac, 1 x 133946 (2)11 Mark Alan Matta, Mattach, Alan Ma
x86 K8 • • • • • • • • • • • • • • • • • •	4166 1 1 8 800000; 1008 AMD ANDIN 56 80001; 101; 101 (2017); 044404
x86 Atom	Marine 3 x 12020945 (200 Mole Allow 2200 Adde
x86 Eden	klaine, 1 x 300096, 2007 Via Edwa U.V. alls Edwa (162); experary-XG
ppc32 G2 +	(2 3 x 300/17 mmsdr PowrQUCC 1 MPCBIBLEDQ080, pmB2 43 (6); opproprint
ppc32 G3	
ppc32 G4	in 1 1 2024b 28 Minish Ameri V 81 11 (b) pro2 4 (b) (b) prop pro-
armeabi Krait	Kaji. 11 14/04/02, 200 Milliola Powerf, Ur Milli, BOUZI, Ur (44), appropriate Managar, 2 i STAMME, Bild Quanteens Generations Sa AF-Q005A, several (14), Atteil, appropriate Managar, 2 i STAMME, Bild Quanteens Generations Sa AF-Q005A, several (14), Atteil, appropriate
armeabi Scorpion	A/
armeabi Cortex A8	NAMERY, 1 & BOROME, 2000 TERMINAL MODEL, 2000 (CARLS), 200

#### Speed comparison of signature systems

a cycrew	ronald4096		rainbow5640				
			<b>Gardoon</b>				
2 <sup>27</sup> cycles	ronald3072	(art) (at a to a	re seresquipinar	y256181212		215	bytes
	<ul> <li>modsig160</li> </ul>		With				
	mogadote /	11554-62	stheirv2	ronald4036	ecclonalde371		
2 <sup>26</sup> cycles	/ rhoosig234	Scp		moair/S072	ecrimal/b/571	-14	bytes
See Okeas	redpiig162	pflasht	/ \\05	1003(02048	ecdonaldp521	- X	0y985
	-ipractors	rosald4096	With .	ronald1536	ecclonalde409		
	renald1536	ronald3072 sflashv2	W03				
2 <sup>25</sup> cycles	spiritowe440	considente	1000	ecidonaldb57	ecclonaldo384	+13	bytes
24- Cycles	Chickey Chickey	ronald1538	100			2.0	<b>Dyoza</b>
	rocald9096 cfbm1	ronald1024	1000	ronald1024	ectionaldk283		
	ronakt9272 spnad1024	r0158d768	1003	ecidonaldk40			
224 cycles			190	ecdonaldb40	9 rwb0lur1024	-012	bytes.
n oyona	ectoraldb571 ecdonald8571 tairbowbinary	16240340/024	ronaid4096	ronald/68	ed25519 ecdonaldo256		0,003
		tronald512	ronac6048	ecoonaidpos hector	ectionaldizes		
			dona/12048	ecdonaldk28	ectonalds233		
2 <sup>23</sup> cycles	eodonardpo21 eodonaldb409 tte6440	.0010izcom.	1003101536	ecdonaldh28	3 ecdonaldo223	011	bytes
	ecdonaldb409, ecdonaldb409 fil90440 ecdonaldb409 ecdonaldb409 fainboebinary	6992 BRANK BR 2018		1 rwb01ur1026	ectionaldp192	-	-,
	edonaldb283 molaid1536 molaid512			1 mode512	annuk/4/205		
		ebbonaldk5	notoralde72	1 ed25519	ronald3072		
2 <sup>22</sup> cycles				ecclonaldo25		210	byons.
	ectional (b)(233 doing to b) (b)	- ecdenaldp6		ecdonaldk23	a roneld1506		
	ecdonaldb233 ecdonaldb233 ecdonaldb234 ecdonaldb2549 ecdonaldb2549	<ul> <li>Ocdenaidk4</li> <li>ocdenaidb4</li> </ul>		ecdonaldb23	3 ronald1024		
	donald2048 rwb04u21024 ecdonald4406	doppendicities	<sup>37</sup> ecdone(s)40	9 ecidonaldo22	1 ronald768		
2 <sup>21</sup> cycles			ecdoral c40	9ecclonaldp19	2 ronald512	- 28	bytes .
		and nonlife 2	ronald763 ecdoneldate	rambow			
		estimate2	ecooreiden	Ins6440 3 tainbow6440	756440		
			ecolorial and	3 taktbow6440	rainbow6440		
2 <sup>20</sup> cycles				3 econade 15	3 ecdonaldk163 3 ecdonaldb163		bytes .
				000120016	255065624081ary25618121		
				excelosed in 16	ectonakto160		
2 <sup>19</sup> cycles	dorekfillpred cotorektp192 ectionaktk222	danald512			decair/2048	27	
2 <sup>10</sup> cycles			Concession of the		dorvaid1024	-24	bytes
	ed25519 ecdonalds163 ecdonalds165				donald512		
		BODDFHECK I	ecoloreldo/2	<ul> <li>rainbowbinar</li> </ul>	#8E48038binary16242020		
2 <sup>18</sup> cycles		0000142001	ecdoreidp19	stister2	6E4008binary16242020 sflashv2	- 28	bytes
2 ··· Cycles		- Conservation in				27	0yours
			ecdoneldb16 ecdoneldp16	pflash1	pflash1		
	migdsk024 heav		ecdonaldp16	aliop	3icp		
2 <sup>17</sup> cycles		hector	ed25519	moosid224	mace/ag256 mace/ag224	25	bytes.
		+ 1995 P.41		mogsig182	magping.com		0,000
	donald512			mogsig160	magsig160		
	•ronald1536 effetting			unddaid 160	audichid ico		
2 <sup>16</sup> cvcles						-24	byons .
,	ed25519 ed25519						.,
2 <sup>15</sup> cycles						23	bytes
	rainbowbinary 16243000 pary 256181212						
2 <sup>14</sup> cycles	rientiowbenary#56181212					22	bytes
	7 W I						
	rwb04u31024						
-12	-Importation*					21	
2 <sup>13</sup> cycles	N 1					-21	bytes
	verification soning key-pair	secret-key	public-key	signature	signed-message		
	cycles cycles cycles	bytes	bytes	bytes.	overhead		

64-bit 2400MHz Intel Xeon E5620



32-bit 1900MHz Pentium 4

Bernstein, Lange: High-speed high-security cryptography on ARMs

# Benchmarking of cryptographic systems

- We benchmark all submitted primitives on more than 100 different CPUs. So far 1112 implementations submitted.
- Cooperating project for smaller CPUs: xbx.das-labor.org.
- Benchmarking framework and all implementations are public. Anybody can run benchmark on own computer (we're happy to post your data!).
- Clear speed differences between security levels.
- Clear speed differences between devices we count cycles to eliminate influence of clock speed but CPUs do different # operations in one clock cycle.
- Clear speed differences between libraries (e.g. OpenSSL much slower than NaCl)
- Clear speed differences between choices within one family, e.g. elliptic-curve speed depends on the representation, the coordinate system, the windowing method, ...

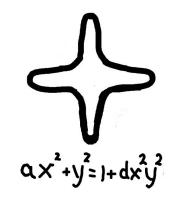
Networking and Cryptography library (NaCl) nacl.cr.yp.to

- ► All cryptography has at least 128-bit security (takes at least 2<sup>128</sup> operations to break).
- Covers
  - authenticated encryption (incl. DH key exchange)
  - signatures
  - both based on elliptic curves for public-key part
- Easy user interface.
- Very good speed.
- Software side-channel attack resistant: all operations take constant time, no key-dependent branches, no key-dependent addresses.
- Implementations are public domain, no known patent issues.
- Biggest early adopter: DNSCrypt from OpenDNS.

# Public-key authenticated encryption

- User interface: crypto\_box, takes public key of recipient, secret key of sender, and a nonce (number used only once)
- Diffie-Hellman key exchange using long-term keys.
- Stream cipher with MAC for bulk encryption.
- Security-optimized speed-optimized choice of cryptographic primitives, more specifically
  - Elliptic curve in twisted Edwards form, conforming to IEEE-P1363, plus additional security properties.
  - Salsa20 stream cipher (from final eSTREAM portfolio).
  - Poly1305 (information-theoretic security).





## Car security as a crypto performance challenge

C 🔇 preserve-project.eu		
PRESE preparing secure v2x commu	RVE	
Home	147.1	
About PRESERVE	Welcome	Consortium
News	Welcome to the webpage of the PRESERVE project.	UNIVERSITY OF TWENTE.
Harmonization Workshop	PRESERVE contributes to the security and privacy of future	
Consortium	vehicle-to-vehicle and vehicle-to-infrastructure communication	escrypt Integand Security
Project Partners	<ul> <li>systems by addressing critical issues like performance, scalability, and deployability of V2X security systems.</li> </ul>	Fraunhofer
Advisory Board	and deployability of v2X security systems.	SIT
Dissemination	Frank Kargl	🗾 Fraunhofer
Deliverables	Scientific Coordinator PRESERVE	AISEC
Scientific Publications		
Presentations		
Press Coverage	News	RENAUT

Bernstein, Lange: High-speed high-security cryptography on ARMs

## Car security as a crypto performance challenge



Bernstein, Lange: High-speed high-security cryptography on ARMs

#### Car security as a crypto performance challenge

PRESERVE deliverable 1.1, "Security Requirements of VSA":

The different driving scenarios we looked into indicate that in most driving situations (SUL, MUL, and SHL) the packet rates do not exceed 750 packets per second. Only the maximum highway scenario (MHL) goes well beyond this value (2,265 packets per second). ...

Processing 1,000 packets per second and processing each in 1 ms can hardly be met by current hardware. As discussed in [32], a Pentium D 3.4 GHz processor needs about 5 times as long for a verification (which is the most time-consuming operation in cryptographic processing overhead) and a typical OBU even 26 times as long. This is a good indication that a dedicated cryptographic co-processor is likely to be necessary.

#### Performance measurement on a large processor

NaCl measurements on typical desktop CPU (4-core 2400MHz Intel Xeon E5620, \$390 last year):

- ► 4.99 cycles/byte for secret-key encryption (Salsa20).
- 2.66 cycles/byte for secret-key authentication (Poly1305).
- ▶ 227348 cycles for public-key session (ECDH: Curve25519).

- ► 272592 cycles to verify a signature (EdDSA: Ed25519).
- ▶ 133593 cycles to verify a signature inside a *batch*.
- 87336 cycles to sign a message.

#### Performance measurement on a large processor

NaCl measurements on typical desktop CPU (4-core 2400MHz Intel Xeon E5620, \$390 last year):

- ► 4.99 cycles/byte for secret-key encryption (Salsa20).
- 2.66 cycles/byte for secret-key authentication (Poly1305).
- ▶ 227348 cycles for public-key session (ECDH: Curve25519).

- ► 272592 cycles to verify a signature (EdDSA: Ed25519).
- ▶ 133593 cycles to verify a signature inside a *batch*.
- 87336 cycles to sign a message.

Let's focus on ECDH: 42000 operations/second.

#### Performance measurement on a large processor

NaCl measurements on typical desktop CPU (4-core 2400MHz Intel Xeon E5620, \$390 last year):

- ► 4.99 cycles/byte for secret-key encryption (Salsa20).
- 2.66 cycles/byte for secret-key authentication (Poly1305).
- ▶ 227348 cycles for public-key session (ECDH: Curve25519).
- ► 272592 cycles to verify a signature (EdDSA: Ed25519).
- ▶ 133593 cycles to verify a signature inside a *batch*.
- 87336 cycles to sign a message.

Let's focus on ECDH: 42000 operations/second.

**90000** operations/second on another typical desktop CPU (3300MHz 6-core AMD Phenom II X6 1100T CPU, \$190 last year).

## Performance measurement on a small processor

BeagleBone development board revision A6: 720MHz TI Sitara AM3359 CPU; ARM Cortex A8 core.

(Picture credits: beagleboard.org)

Our public-key speed:



## Performance measurement on a small processor

BeagleBone development board revision A6: 720MHz TI Sitara AM3359 CPU; ARM Cortex A8 core.

(Picture credits: beagleboard.org)

Our public-key speed: **1447** ECDH/second. Fully protected against software side-channel attacks.



・ロト ・ 日 ・ ・ 日 ・ ・ 日 ・ ・ 日

#### Performance extrapolation

Faster Cortex A8 cores are widely used in mobile devices:

- 1000MHz Apple A4 in iPad 1, iPhone 4 (2010);
- 1000MHz Samsung Exynos 3110 in Samsung Galaxy S (2010);

- 1000MHz TI OMAP3630 in Motorola Droid X (2010);
- 800MHz Freescale i.MX50 in Amazon Kindle 4 (2011);

etc.

Our tests on various Cortex A8 cores demonstrate that performance is almost exactly linear in clock speed.

#### Performance extrapolation

Faster Cortex A8 cores are widely used in mobile devices:

- 1000MHz Apple A4 in iPad 1, iPhone 4 (2010);
- 1000MHz Samsung Exynos 3110 in Samsung Galaxy S (2010);
- 1000MHz TI OMAP3630 in Motorola Droid X (2010);
- 800MHz Freescale i.MX50 in Amazon Kindle 4 (2011);
- etc.

Our tests on various Cortex A8 cores demonstrate that performance is almost exactly linear in clock speed.

Reasonably safe ECDH extrapolations to other Cortex A8 cores:

- ▶ 1200/second: 600MHz TI AM3352ZCZ60, 13.5€ (DigiKey).
- > 2400/second: 1200MHz Allwinner A10, reportedly \$7.

But always better to measure directly. We're working on it!