Répás Sándor[242]: *ARM alapú mikroszámítógépek titkosítási képességeinek vizsgálata*

Absztrakt: A Raspberry Pi 2012-es megjelenése óta eltelt néhány év alatt számtalan ARM architektúrára épülő mikroszámítógép jelent meg. Ezek elterjedésével Linux futtatására alkalmas, költséghatékony eszközök váltak széles körben is hozzáférhetővé. Méretükhöz, valamint fogyasztásukhoz viszonyított magas teljesítményüknek, valamint az elterjedt Linux operációs rendszer futtatásának köszönhetően előnyösen alkalmazhatóak sok feladat esetén. Kiemelkedően fontos terület az információbiztonság. Az információbiztonság szinte minden területén fontos szerep jut a különböző titkosítási, kódolási algoritmusoknak. Ugyanakkor ezek az algoritmusok rendkívül számításigényesek, így fontos annak vizsgálata, hogy mely mikroszámítógépek, milyen kompromisszumok mellett alkalmazhatóak ezekre a feladatokra. Megvizsgálásra és bemutatásra kerül tíz különböző mikroszámítógép teljesítménye elterjedt, szimmetrikus, valamint publikus kulcsú kódoló és dekódoló, valamint lenyomatképző és üzenethitelesítő protokoll alkalmazása esetén: RSA, AES, HMAC, MD5, SHA. A megbízható titkosításhoz elengedhetetlenül szükség van megbízható (ál)véletlen számok előállítására, ugyanakkor az ARM SoC-okra épülő mikroszámítógépek általában rendelkeznek hardveresen magvalósított (ál)véletlenszám-generátorokkal. Megvizsgálásra és bemutatásra kerül a különböző mikroszámítógépek véletlenszám-generátorának alkalmazhatósága, valamint ismertetésre kerülnek az alkalmazott vizsgálati módszerek is, valamint ajánlások megfogalmazására is sor kerül.

Bevezetés

A félvezető technológiák folyamatos fejlődésének következményeként egyre alacsonyabb költségekkel előállítható, egyre alacsonyabb energiafelhasználás mellett egyre nagyobb teljesítményt nyújtó mikroprocesszorok és mikrokontrollerek jelentek meg. Az integráltság fokának növekedésével pedig lehetővé vált olyan félvezető lapkák előállítása is, melyek együtt tartalmazzák mind a mikroprocesszort, mind pedig az azt kiegészítő áramköröket (pl: memóriavezérlők, grafikus vezérlők, USB vezérlők, stb.). Ezen félvezető lapkák (System on a Chip, SoC) segítségével kerülnek előállításra az egyre népszerűbb okos telefonok, az okos telefonkészülékek népszerűsége pedig gyorsítja a lapkák fejlődését is. A mind nagyobb teljesítményű SoC-ok lehetővé tették az egykártyás mikroszámítógépek (Single Board Computer, SBC) megjelenését is, melyekből a legismertebb a 2012-ben megjelent, ARM architektúrára épülő [1], egy magos 700 MHz-es processzorral, 256 MB memóriával rendelkező Raspberry Pi [2]. A gyors fejlődésnek köszönhetően ma már nyolc magos processzorral és 2GB memóriával ellátott SBC is elérhető [3].

Napjainkban egyre fontosabb szerep jut az információbiztonságnak, melynek kiemelkedően fontos területei a kódolás, dekódolás, titkosítás, digitális aláírás és az aláírás ellenőrzése. Ugyanakkor a titkosítással kapcsolatos műveletek rendkívül nagy számítási igénnyel rendelkező matematikai műveletek. Az egyre nagyobb teljesítményű, ugyanakkor költséghatékony SBC-k elterjedése miatt fontos kérdés, hogy az SBC-k milyen titkosítási képességekkel rendelkeznek, ezáltal milyen hatékonyan alkalmazhatóak az információbiztonság területén.

A következőkben az SBC-k titkosítási képességeinek vizsgálata során alkalmazott módszereinket és eredményeinket mutatjuk be részletesen.

[242] Óbudai Egyetem, Biztonságtudományi Doktori Iskola, Ph-d hallgató rsandor@ahol.co.hu

Korábbi eredmények

Rengeteg Raspberry Pivel, és egyéb SBC-vel közvetlenül, vagy közvetve foglalkozó publikáció jelent meg.
[4]-ben a szerzők más eredményeik mellett bemutatják a Raspberry Pihez fejlesztett megoldásukat is, melynek segítségével biztonságos TFTP (Secure Trivial File Transfer Protocol) készíthető, amely biztosítja a távolról végezhető frissítések biztonságát. Kutatók vizsgálták a BeagleBone Black [5], a BeagleBone és a Raspberry Pi típusú SBC-k teljesítményét LMbench [6], valamint a saját fejlesztésű (a korlátozott eszközökön alkalmazott CoAP, Constrained Application Protocol) teljesítményt mérő alkalmazásukkal [7]. Arra a következtetésre jutottak, hogy az SBC-k kisebb, mint fele sebességűek, mint egy modern számítógép, míg a legkisebb késleltetéssel a három eszköz közül a BeagleBone Black rendelkezett. Fontos következtetésük, hogy IOT alkalmazások esetében a gyorsabb és drágább külső memória lényegesen kevésbé hat egy SBC teljesítményére, mint a processzor típusa. Ugyanakkor a grafikus felület futása sem befolyásolta számottevően a teljesítményt. Két publikációban mutatták be négy különböző ARM platform memória és processzor teljesítmény vizsgálatának eredményeit kutatók [8] és [9]-ben. Mérési eredményeiket összevetették az Intel Atom [10] processzorok adataival is, melyek hasonló értékeket produkáltak, ugyanakkor az ARM SoC-ra épülő eszközök energiafelhasználása lényegesen alacsonyabb volt. A szerzők is rámutatnak, hogy ez a jövőben megváltozhat. BeagleBoard és PandaBoard [11] segítségével vizsgálták meg kutatók az ARM SoC-ra épülő eszközök használatának lehetőségeit HPC (High Performance Computing) alkalmazásokban [12]-ben, különös tekintettel a számítási teljesítményre és az energiafelhasználásra. A szerzők arra a következtetésre jutottak, hogy a HPC alkalmazások szempontjából felesleges eszközök (pl. USB, HDMI, VGA, stb.) nagy energiafelhasználása miatt HPC kialakítások esetében nem jól alkalmazhatóak az általános SoC-okra épülő SBC-k. [13]-ban a szerzők hat különböző típusú SBC-t több szempontból vizsgáltak meg, azzal a céllal, hogy kiderítsék, hogy a különböző SBC-kből épített heterogén klaszter párhuzamosan végrehajtott diszkrét idejű szimulációk [14] során milyen teljesítményt produkál. Fontos eredményük, hogy a számításoknál elsődlegesen a többmagos teljesítmény figyelembevétele hoz valós eredményeket. A publikációk nem vizsgálják az SBC-k titkosítással kapcsolatos műveletek során produkált teljesítményét, így szükség van ennek mérésére alkalmas módszerek kidolgozására és a vizsgálatok elvégzésére.

Vizsgálati módszerek
A következőkben bemutatjuk a vizsgálatok elvégzésére kiválasztott eszközöket, valamint az alkalmazott vizsgálati módszereket.

Eszközök kiválasztása
Az eszközök kiválasztása során elsődlegesen a következő szempontokat vettük figyelembe:

- Elterjedtsége miatt a Raspberry Pi vizsgálata feltétlenül szükséges, hiszen nagymértékben növeli az eredmények felhasználhatóságát.
- Minél többféle SoC mérése történjen meg, ezáltal átfogó képet nyújtva az egyes SoC-ok összehasonlításához.

Táblázat 1: Vizsgált SBC-k legfontosabb paraméterei

Típus	CPU architektúra	SoC típus	CPU mag. (db)	CPU frekv. (GHz)	RAM méret (GB)
Banana Pi	Cortex A7	AllWinner A20	2	1	1
Banana Pi M2	Cortex A7	AllWinner A31s	4	1	1

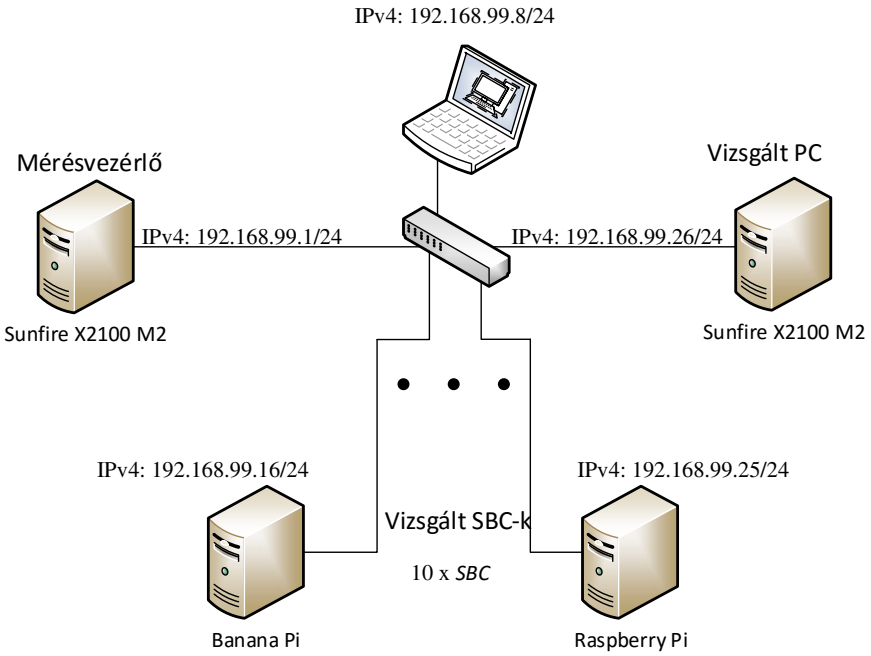
BeagleBone Black	Cortex A8	TI AM3359	1	1	0,5
ODROID-C1	Cortex A5	Amlogic S805	4	1,5	1
ODROID-U3	Cortex A9	Samsung Exynos 4412	4	1,7	2
ODROID-XU3 Lite	Cortex A15+A7	Samsung Exynos 5422	4+4	1,8+1,3	2
Orange Pi Mini	Cortex A7	AllWinner A20	2	1	1
Orange Pi Plus	Cortex A7	AllWinner H3	4	1,6	1
Raspberry Pi Model B+	1176JZ(F)-S	Broadcom BCM2835	1	0,7	0,5
Raspberry Pi 2 Model B+	Cortex A7	Broadcom BCM2836	4	0,9	1

- Szerepeljen a vizsgálatokban két eltérő gyártótól származó SBC, melyek ugyanolyan SoC-ra épülnek. Ezáltal kiderülhessen, hogy a produkált teljesítmény mennyire a SoC-tól, és mennyire a SoC mellé került elemektől (pl: memória) függ.
- Megvizsgálásra kerüljön legalább egy Big-Little architektúrát alkalmazó SoC-ra épülő SBC. Így kiderüljön, hogy milyen előnyei és hátrányai lehetnek egy ilyen SoC alkalmazásának.

Mérési környezet

A vizsgálatok elvégzéséhez az összes SBC eszközön Linux került telepítésre. Amennyiben a gyártó ad, vagy ajánl Linux verziót az eszközhöz, úgy azt alkalmaztuk. Minden esetben arra törekedtünk, hogy csak a legszükségesebb változtatásokat hajtsuk végre, minden, a teljesítményt befolyásoló módosítást elkerüljünk. Ez alól egyetlen kivétel, hogy minden eszközön letiltottuk a grafikus felület indítását, hogy az ne befolyásolja a mérési eredményeket.

A mérések elvégzéséhez az 1. ábrán látható hálózat kivitelezésére volt szükség. Az ábra tetején elhelyezkedő laptopról került indításra a mérési folyamat, és annak előrehaladását is innen lehetett ellenőrizni. Az ábra bal szélén elhelyezkedő szerver vezérelte le a mérést, gyűjtötte össze, majd előzetesen feldolgozta az adatokat. Az ábra alján szerepel a tíz vizsgált SBC. Az összehasonlíthatóság érdekében minden mérést elvégeztünk az ábra jobb oldalán látható Sun Sunfire X2100 M2 típusú számítógépen is, mely Opteron 1222 dual core CPU-t, és 4 darab 2GB DDR2-5300 ECC RAM modult tartalmazott.



Ábra 1: A vizsgálatok elvégzéséhez kialakított környezet

Mérések és eredmények

A pontos eredmények érdekében a méréseket BASH scriptek segítségével automatizálva végeztük el. Minden mérést, egymás után 16 alkalommal megismételve, melyből csak az utolsó 11 alkalom eredményei kerültek feldolgozásra. Ezáltal elkerülhetővé vált a háttértár sebességének befolyásoló hatása a mérések során (a cache alkalmazásával). A mérésekhez az openssl speed parancsát, valamint más openssl parancsokat használtunk. Ahol értelmezhető, ott a méréseket egy, majd az összes mag felhasználásával is elvégeztük. A méréseket a Sunfire X2100 M2 számítógépen is elvégeztük, ezáltal megkönnyítve az összevetést. Az eredményeket szöveges állományokba gyűjtöttük, majd az elő-feldolgozást awk scriptekkel, majd a kiértékelést Microsoft Excel segítségével végeztük el. A következőkben részletesen ismertetjük a mérési eredményeket, majd részletesen kiértékeljük azokat.

Szimmetrikus kulcsú titkosítás

Napjaink legelterjedtebb szimmetrikus kulcsú titkosítása a Rijndael algoritmust alkalmazó Advanced Encryption Standard (AES) [14]. Használják 128, 192 és 256 bites hosszú kulcs segítségével is. Felhasználása nagyon széleskörű. A vizsgálatok során az állománytitkosítás során mutatott teljesítményét vizsgálatuk, Cipher Block Chaining (CBC) módban, mely mód alkalmazása nagymértékben megnöveli az algoritmikus támadással szembeni védelmet.

A méréseket az openssl speed parancs segítségével, mindhárom kulcshosszal, 8k blokkmérettel, 1 majd több szálon is elvégeztük. A több szál alkalmazásával lehetővé vált a több CPU mag egyidejű igénybevétele.

Eredmények egy szál esetén

A futtatások során keletkezett eredmények átlagát a 2. táblázat, míg a szórások értékét a 3. táblázat tartalmazza. Az átlagokat grafikusan is ábrázoltuk a könnyebb áttekinthetőség érdekében a 2. ábrán.

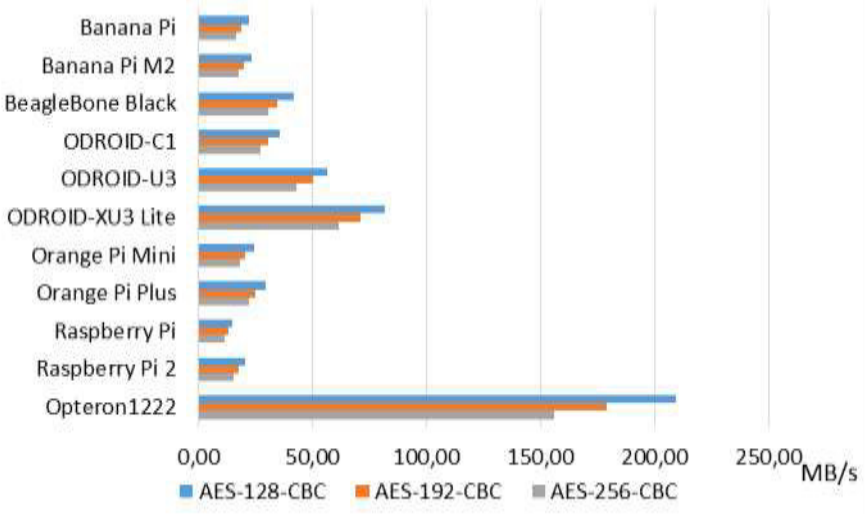
A 2. táblázat első oszlopa tartalmazza a vizsgált SBC típusát. A második oszlop a másodpercenként kódolt adatok mennyiségének átlagát MB-ban 128 bites kulcshosszú AES CBC (AES-128-CBC) alkalmazása esetén. A harmadik oszlop az AES-192-CBC, míg az utolsó az AES-256-CBC alkalmazása során másodpercenként kódolt adatmennyiségek átlagát tartalmazza. A 3. táblázat megfelelő oszlopai a számított átlagértékekhez tartozó szórás értékeket tartalmazzák.

Táblázat 2: AES-CBC kódolás átlagos sebesség (MB/s), 1 szálon, 8k blokkmérettel

Típus	AES-128	AES-192	AES-256
Banana Pi	22,06	18,88	16,60
Banana Pi M2	23,15	19,74	17,49
BeagleBone Black	41,85	34,70	30,82
ODROID-C1	35,95	30,86	27,26
ODROID-U3	56,59	50,44	43,27
ODROID-XU3 Lite	81,85	71,05	61,77
Orange Pi Mini	24,45	20,81	18,33
Orange Pi Plus	29,72	25,32	22,29
Raspberry Pi Model B+	15,06	13,04	11,50
Raspberry Pi 2 Model B+	20,62	17,58	15,59
Opteron 1222	209,50	179,08	156,01

Táblázat 3: AES-CBC sebességek szórása (MB/s), 1 szálon, 8k blokkmérettel

Típus	AES-128	AES-192	AES-256
Banana Pi	0,04	0,03	0,03
Banana Pi M2	0,07	0,04	0,04
BeagleBone Black	0,08	0,06	0,05
ODROID-C1	0,20	0,16	0,14
ODROID-U3	0,48	0,42	0,37
ODROID-XU3 Lite	0,07	0,01	0,03
Orange Pi Mini	0,04	0,08	0,05
Orange Pi Plus	0,03	0,00	0,00
Raspberry Pi Model B+	0,00	0,00	0,00
Raspberry Pi 2 Model B+	0,01	0,03	0,01
Opteron 1222	0,13	0,09	0,07



2. ábra: AES-CBC kódolás átlagos sebesség (MB/s), 1 szálon, 8k blokkmérettel futtatva

Eredmények értékelése
Az értékek vizsgálata alapján kijelenthető, hogy:

- A leggyorsabb az Odroid-XU3 Lite, második az Odroid-U3, míg a harmadik a BeagleBone Black.
- Leglassabb a Raspberry Pi.
- A két azonos SoC-ra épülő SBC eltérő eredményeket produkált (Banana Pi és Orange Pi Mini), azonban ez az eltérés csak 10% körüli.
- A szórás értékek az átlagértékekhez viszonyítva alacsonyak, így a mért értékeket stabilan produkálják a vizsgált eszközök.
- Az egyes SBC-k egymáshoz viszonyított teljesítményét nem befolyásolja számottevően a kódolás során alkalmazott kulcshossz.
- Még a leggyorsabb SBC sebessége is töredéke az Opteron 1222 alapú rendszernek (pl: AES-128-CBC esetén: 209,5/81,85=2,56).

Eredmények több szál esetén
A több szálas futtatásokat olyan SoC-okra épülő SBC-k vizsgálatánál alkalmaztuk, melyek több processzormagot is tartalmaznak. A mérést minden esetben annyi szálon végeztük el, ahány maggal az adott SoC-ban lévő processzor rendelkezik, ezáltal a mérés során minden mag részt vett a kódolásban, és az összesített teljesítményt mérhettük. A Big-Little architektúrát alkalmazó Odroid-XU3 Lite esetén az eltérő magsebességek miatt a mérést elvégeztük 4 szál használatával is. Az eredmények bemutatásához az AES-256-CBC kódolás eredményeit emeltük ki, melyeket a 4. táblázat tartalmaz.
A második oszlop mutatja, hogy az adott mérés hány szál segítségével történt. A harmadik oszlop a kódolt adatok átlagsebességét mutatja a 11 utolsó mérésből. A negyedik oszlopban lévő adatok az egy szálas mérésnél már ismertetésre kerültek, itt csak a könnyebb átláthatóság miatt kerültek újra bemutatásra.

Táblázat 4: AES-256-CBC eredmények, több szálon, 8k blokkmérettel

Típus	Szálak	AES-256-CBC X szál (MB/s)	AES-256-CBC 1 szál (MB/s)	Relatív gyorsulás	Szórás
Banana Pi	2	33,22	16,60	2,00	0,02
Banana Pi M2	4	69,96	17,49	4,00	0,02
ODROID-C1	4	109,57	27,26	4,02	0,04
ODROID-U3	4	88,43	43,27	2,04	7,38
ODROID-XU3 Lite	4	195,01	61,77	3,16	1,01
ODROID-XU3 Lite	8	276,21	61,77	4,47	2,20
Orange Pi Mini	2	36,36	18,33	1,98	0,01
Orange Pi Plus	4	46,55	22,29	2,09	6,40
Raspberry Pi 2	4	62,31	15,59	4,00	0,01
Opteron 1222	2	310,88	156,01	1,99	0,32

Az 5. oszlopban mutatott relatív gyorsulás a negyedik és a harmadik oszlopban szereplő átlagsebességek aránya. Az utolsó oszlop tartalmazza a harmadik oszlophoz tartozó szórás értékeket.

Eredmények értékelése
Az értékek vizsgálata alapján kijelenthető, hogy:

- A leggyorsabb az Odroid-XU3 Lite, második az Odroid-C1, míg a harmadik az Odroid-U3.

- Az Odroid-XU3 Lite, Odroid-U3, valamint az Orange Pi Plus eredményei nagy szórásértékeket mutatnak. A mért teljesítmény nem állandó, nagy eltéréseket mutat, nem kiszámítható a rendszer viselkedése.
- Alacsony szórásértékeket produkáló eszközök közül a leggyorsabb SBC az Odroid-C1, Banana Pi M2, valamint a Raspberry Pi 2.
- A relatív gyorsulás a három magas szórást produkáló eszköz kivételével közel azonos az igénybevett processzormagok számával. A magok számának növelésével lineárisan arányos gyorsulás érhető el.
- A leggyorsabb SBC teljesítménye nyolc mag használatával már megközelíti az Opteron 1222 rendszer teljesítményét.

Lenyomatképzés és üzenethitelesítés

A lenyomatképzők (hash) és hitelesítők alkalmazása szintén elengedhetetlen a biztonságos kommunikáció biztosításához. Alkalmazásuk célja általában a sértetlenség biztosítása, a sérülés detektálása. A vizsgált protokollok, és néhány jellemzőjük:

- MD5
  - 128 bit hosszú hash,
  - Alkalmazása nem biztonságos, de régi kompatibilitási okokból előfordul.
- SHA1
  - 160 bit hosszú hash,
  - Alkalmazása már szintén nem ajánlott,
  - Széles körben elterjedt, ismert és használt.

- SHA256
  - 256 bit hosszú hash,
  - Alkalmazásra javasolt.
- SHA512
  - 512 bit hosszú hash,
  - Lassúsága miatt alkalmazása nem minden esetben javasolt.
- HMAC
  - MD5 alapú üzenethitelesítő
  - Keyed-Hash Message Authentication Code

Eredmények egy szál esetén

A futtatások során keletkezett eredmények átlagát az 5. táblázat, míg a szórások értékét a 6. táblázat tartalmazza. Az átlagokat grafikusan is ábrázoltuk a könnyebb áttekinthetőség érdekében a 3. ábrán.
A táblázat felépítése nagyon hasonló a korábbi táblázatok esetében alkalmazottakhoz, így nem ismertetjük részletesen.

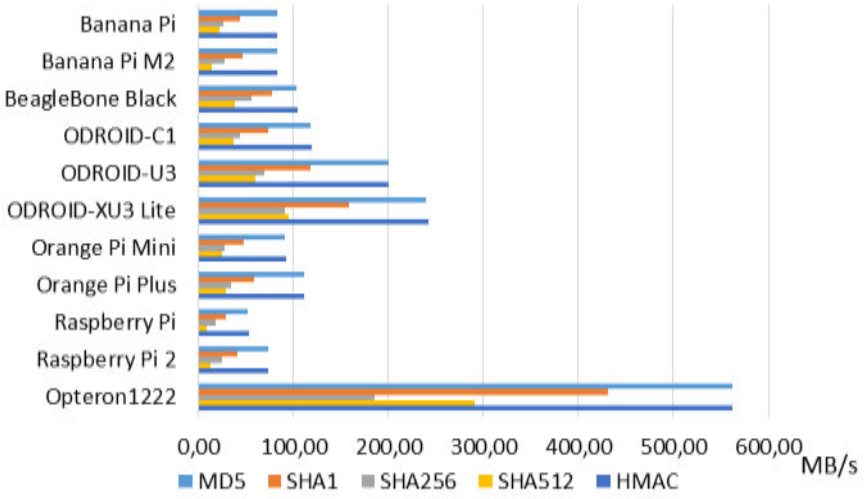
Táblázat 5:Lenyomatképző és üzenethitelesítő átlageredmények, egy szálon, 8k blokkmérettel

Típus	MD5	SHA1	SHA256	SHA512	HMAC
Banana Pi	82,49	44,29	26,01	22,35	82,62
Banana Pi M2	82,96	46,30	27,93	14,12	82,83
BeagleBone Black	102,88	77,57	56,30	37,88	104,70
ODROID-C1	118,71	73,62	43,43	36,66	118,88
ODROID-U3	200,43	118,47	69,70	59,88	200,17
ODROID-XU3 Lite	240,15	158,88	91,43	95,70	242,87
Orange Pi Mini	91,53	48,22	28,33	24,41	91,90
Orange Pi Plus	111,43	58,67	34,52	29,69	111,98

Raspberry Pi	51,92	29,12	18,79	9,11	53,15
Raspberry Pi 2	73,77	41,19	24,84	12,56	73,65
Opteron 1222	562,56	430,60	186,18	290,29	562,81

Táblázat 6: Lenyomatképző és üzenethitelesítő szórások, egy szálon, 8k blokkmérettel

Típus	MD5	SHA1	SHA256	SHA512	HMAC
Banana Pi	0,23	0,11	0,05	0,02	0,16
Banana Pi M2	0,13	0,11	0,04	0,03	0,17
BeagleBone Black	0,08	0,10	0,09	0,07	0,15
ODROID-C1	0,72	0,37	0,23	0,19	0,69
ODROID-U3	2,05	1,21	0,68	0,54	1,80
ODROID-XU3 Lite	0,18	0,25	0,14	0,08	0,20
Orange Pi Mini	0,53	0,47	0,05	0,02	0,20
Orange Pi Plus	0,03	0,01	0,00	0,00	0,08
Raspberry Pi	0,10	0,01	0,03	0,00	0,03
Raspberry Pi 2	0,08	0,03	0,06	0,01	0,15
Opteron 1222	1,11	0,17	0,85	0,08	0,71



3. ábra: Lenyomatképzés és üzenethitelesítés átlagos sebesség (MB/s), 1 szálon, 8k blokkmérettel futtatva

Eredmények értékelése

Az értékek vizsgálata alapján kijelenthető, hogy:

- A leggyorsabb az Odroid-XU3 Lite, második az Odroid-U3. MD5 és HMAC esetében harmadik az Odroid-C1, a többi esetben a BeagleBone Black.
- Leglassabb a Raspberry Pi.
- A két azonos SoC-ra épülő SBC eltérő eredményeket produkált (Banana Pi és Orange Pi Mini), azonban ez az eltérés itt is csak 10% körüli.
- A szórás értékek az átlagértékekhez viszonyítva alacsonyak, így a mért értékeket stabilan produkálják a vizsgált eszközök.

- Az egyes SBC-k egymáshoz viszonyított teljesítményei nem feltétlenül egyeznek meg az eltérő feladatok esetén (pl: Odroid-C1 és BegaleBone Black MD5 estén: 118,71/102,88=1,15, míg SHA1 esetén: 73,62/77,57=0,95).
- Még a leggyorsabb SBC sebessége is töredéke az Opteron 1222 alapú rendszernek (pl: MD5 esetén: 562,56/240,15=2,34, míg SHA512 esetén: 290,29/95,70=3,03).

Eredmények több szál esetén

Az eredmények bemutatásához elterjedtsége miatt az SHA256 hash képzés eredményeit emeltük ki, melyeket a 7. táblázat tartalmaz. A táblázat felépítése megegyezik a 4. táblázatéval.

Táblázat 7: SHA256 eredmények, több szálon, 8k blokkmérettel

Típus	Szálak	SHA256 X szál (MB/s)	SHA256 1 szál (MB/s)	Relatív gyorsulás	Szórás
Banana Pi	2	52,04	26,01	2,00	0,08
Banana Pi M2	4	111,79	27,93	4,00	0,13
ODROID-C1	4	174,79	43,43	4,02	0,21
ODROID-U3	4	260,81	69,70	3,74	112,01
ODROID-XU3 Lite	4	317,19	91,43	3,47	6,99
ODROID-XU3 Lite	8	442,94	91,43	4,84	31,49
Orange Pi Mini	2	56,32	28,33	1,99	0,13
Orange Pi Plus	4	72,00	34,52	2,09	32,10
Raspberry Pi 2	4	99,54	24,84	4,01	0,09
Opteron 1222	2	370,94	186,18	1,99	1,72

Eredmények értékelése

Az értékek vizsgálata alapján kijelenthető, hogy:

- A leggyorsabb az Odroid-XU3 Lite, második az Odroid-U3, míg a harmadik az Odroid-C1.
- Az Odroid-XU3 Lite, Odroid-U3, valamint az Orange Pi Plus eredményei nagy szórásértékeket mutatnak. A mért teljesítmény nem állandó, nagy eltéréseket mutat, nem kiszámítható a rendszer viselkedése.
- Alacsony szórásértékeket produkáló eszközök közül a leggyorsabb SBC az Odroid-C1, Banana Pi M2, valamint a Raspberry Pi 2.
- A relatív gyorsulás a három magas szórást produkáló eszköz kivételével közel azonos az igénybevett processzormagok számával. A magok számának növelésével lineárisan arányos gyorsulás érhető el.

Nyilvános kulcsú titkosítás

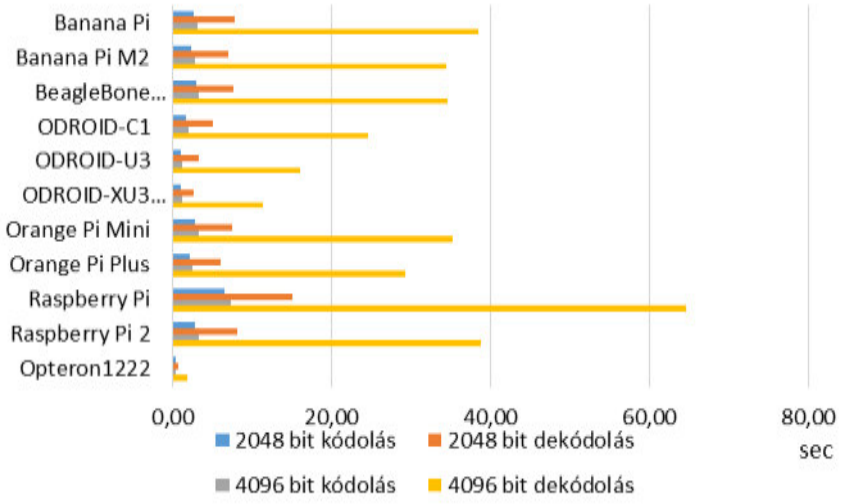
A nyilvános kulcsú titkosítást általában szimmetrikus kulcsok titkosított továbbítására, digitális aláírás hitelesítésére alkalmazzák. A jelenleg használt módszerek rendkívül számításigényesek, és lassúak, így nagymennyiségű adat továbbítására általában szimmetrikus titkosítással kombináltan használják. A vizsgálatok során a jelenleg legelterjedtebb, Ron Rivest, Adi Shamir, Leonard Adleman által kidolgozott RSA kódolást vizsgáltuk 2048 és 4096 bit hosszú kulcsokkal, mivel a megfelelő biztonság érdekében jelenleg minimálisan a 2048 bites kulcshossz alkalmazása ajánlott.

RSA kódolás eredmények

Az RSA kódolás során minden SBC esetében ugyanazt a véletlenszerűen előállított állományt, ugyanazzal a kulcspárral kódoltuk és dekódoltuk. A 2048 bites kulcs segítségével történő kódolás teljesítményének vizsgálatához 1920 bites, míg a 4096 bites kulcshoz 4000 bites állományokat kódoltunk, vagy dekódoltunk minden mérési ciklusban 100 alkalommal. A vizsgálat eredményeit a 8. táblázat tartalmazza, míg grafikusan a 4. ábrán jelenítettük meg azokat.

Táblázat 8: 100 darab RSA kódolás és dekódolás átlagos ideje másodpercben

Típus	2048 bit kódolás	2048 bit dekódolás	4096 bit kódolás	4096 bit dekódolás
Banana Pi	2,71	7,89	3,14	38,54
Banana Pi M2	2,43	7,07	2,82	34,42
BeagleBone Black	3,03	7,68	3,42	34,58
ODROID-C1	1,74	5,05	2,02	24,56
ODROID-U3	1,10	3,30	1,28	16,12
ODROID-XU3 Lite	1,18	2,73	1,31	11,41
Orange Pi Mini	2,88	7,62	3,28	35,33
Orange Pi Plus	2,22	6,16	2,55	29,27
Raspberry Pi	6,63	15,19	7,36	64,64
Raspberry Pi 2	2,93	8,15	3,37	38,84
Opteron 1222	0,50	0,74	0,52	1,89



4. ábra: 100 darab RSA kódolás és dekódolás átlagos ideje másodpercben

Eredmények értékelése

Az értékek vizsgálata alapján kijelenthető, hogy:

- Kódolások esetén leggyorsabb az Odroid-U3, második az Odroid-XU3 Lite, míg dekódolásoknál a sorrend felcserélődik. Harmadik minden esetben az Odroid-C1.
- Leglassabb a Raspberry Pi.

- A két azonos SoC-ra épülő SBC eltérő eredményeket produkált (Banana Pi és Orange Pi Mini), a kódolás végrehajtásánál a Banana Pi volt gyorsabb, míg a dekódolások műveleténél az Orange Pi Mini. A különbségek a két SoC esetében minden esetben 10% alatt maradtak.
- Az egyes SBC-k egymáshoz viszonyított teljesítményei nem feltétlenül egyeznek meg az eltérő feladatok esetén.
- Még a leggyorsabb SBC sebessége is töredéke az Opteron 1222 alapú rendszernek (Pl: 4096 bit kulcshossz dekódolás esetén: 11,41/1,89=6,04).

Véletlen számok generálása

A véletlen számoknak és előállításuknak a kriptográfiában kiemelt szerep jut. Megfelelő véletlen szám nélkül nem végezhető biztonságos titkosítás sem. Valós véletlen számok (TRN) előállítása számítógépekkel szinte lehetetlen. Álvéletlen számok (PRN) előállítására több algoritmus is ismert, melyek más és más célokra ajánlottak. Néhány kifejezetten nem ajánlott titkosítási feladatokhoz, míg más célokra megfelelőek (Pl: Dual_EC_DRBG).

A fellelhető információk szerint (szinte) mindegyik vizsgált ARM alapú SoC rendelkezik valamilyen hardveres véletlen szám generátorral (HWRNG). A következő információk a nyilvánosan hozzáférhető dokumentációkból kerültek kiemelésre:

- Amlogic S805: Built-in LSFR Random number generator.
- TI AM3359: Crypto Hardware Accelerators (AES, SHA, PKA, RNG).
- Allwinner A20: 160-bit hardware PRNG with 192-bit seed.
- Allwinner A31: 160-bit hardware PRNG with 192-bit seed.
- Allwinner H3: 160-bits hardware PRNG with 175-bits seed. 256-bits TRNG.
- Samsung Exynos 5422: Hardware Crypto Accelerators: AES, DES/3DES, ARC4, SHA-1/SHA-256/MD5/HMAC/PRNG, TRNG, PKA, and Secure Key Manager.

A két Broadcom által gyártott SoC-ban is található valamilyen HWRNG, azonban erről dokumentációt nem sikerült fellelni.

Támogatás

Egyik vizsgált SoC esetében sincs megfelelően dokumentálva a HWRNG. Csak részleges információkat sikerült találni.

Az összes Allwinner gyártmányú SoC HWRNG-hez készül egy közös Linux driver, azonban a vizsgálatok elvégzésekor ez még nem működött megbízhatóan.

A Samsung által gyártott SoC-okhoz nem sikerült információt fellelni.

A TI AM3359 SoC HWRNG-jét az új kernelek támogatják, azonban a BeagleBone Black-hez kiadott Linuxban még nem ez a kernel van.

Az Odroid-C1-ben lévő Amlogic S805 támogatott.

A Raspberry Pikben megtalálható két Broadcom SoC szintén támogatott.

Vizsgálatok

Entrópia

A dokumentációk hiányosságai miatt csak korlátozottan tudtuk vizsgálni a véletlen számok minőségét: a generált (ál)véletlen számokon csak statisztikai analízist végeztünk. Statisztikai analízishez a legelterjedtebben használt eszközök, valamint legfrissebb verzióik a következők:

- Diehard
- Dieharder 3.31.1
- NIST Special Publication 800-22rev1a 2.1.2
- Ent
- rngtest
- TestU01 1.2.3
- Practically Random 0.92

A vizsgálatok elvégzéséhez 10GB (ál)véletlen szám került előállítására, majd elemzésre. Az elemzések eredményét a 9. táblázat foglalja össze.

Táblázat 9: Generált véletlen számok statisztikai elemzésének eredménye

Típus	Dieharder	Ent X^2 eloszlás	NIST 800-22
ODROID-C1	Rendben	gyanús (98,71%)	1 hiba
Raspberry Pi	1 gyenge (bitstream)	Ok (59,7%)	Rendben
Raspberry Pi 2	1 gyenge (rank 32x32)	szinte gyanús (90,83%)	1 hiba

Az eredmények alapján egyik rendszer által előállított véletlen szám sem használható megnyugtatóan titkosításra. Ugyanakkor a Linux kernelt felkészítették arra, hogy a véletlen számok előállítása során több forrást is felhasználjon, így egy forrás gyengesége még nem feltétlenül okoz problémát, viszont a HWRNG alkalmazása képes felgyorsítani a véletlen számok előállítását. Fontos azt is megjegyezni, hogy a megfelelő dokumentáltság (ezáltal az adott SoC HWRNG működésének ismeretének) hiánya szintén a titkosítási alkalmazások során történő alkalmazás ellen szól.

Vizuális elemzés

Inkább csak érdekességként vizuálisan is megvizsgáltuk az előállított véletlen számok minőségét. Az 5. ábrán láthatóak a generált véletlen számokból előállított képek. Az ábrákat tüzetesen megvizsgálva sem fedezhetünk fel semmilyen rendellenes ismétlődést, alakzatot.

5. ábra: Odroid-C1, Raspberry Pi, valamint Raspberry Pi 2 által előállított véletlen számokból generált képek

Sebesség

A 10. táblázat tartalmazza a HWRNG segítségével történt véletlen szám generálásának sebességét a három vizsgált SBC esetében.

Táblázat 10: HWRNG segítségével előállított véletlen számok generálásának sebessége

Típus	NIST 800-22
ODROID-C1	7,3MB/s
Raspberry Pi	105kB/s
Raspberry Pi 2	147kB/s

Következtetések

Az eredmények alapján kijelenthető, hogy egy átlagos alkalmazás során szükséges titkosítási feladat elvégzésére még a leglassabb SBC teljesítménye is elegendő, azonban a speciálisabb, nagyobb forgalmat bonyolító, vagy titkosítási célfeladatok elvégzésére használt SBC esetében már figyelembe kell venni az egyes SBC-k jellemzőit.

Ha a felhasználási terület miatt csak egy processzor mag használható ki hatékonyan, akkor mutatott teljesítménye alapján a BeagleBone Black alkalmazása ajánlott.

Az Odroid-XU3 Lite, Odroid-U3, valamint az Orange Pi Plus alkalmazása nagy terhelés esetén produkált kiszámíthatatlan működése miatt kerülendő. Az okok kiderítésére további vizsgálatok elvégzését tartjuk szükségesnek.
Teljesítménye és kiszámítható, stabil működése miatt titkosítási alkalmazásokhoz javasoljuk az Odroid-C1 használatát (ráadásul HWRNG-je is a leggyorsabb a vizsgált eszközök között). Sebessége miatt jó választás még a Bana Pi M2 is. Elterjedtsége, és ezáltal támogatottsága és ismertsége miatt a Raspberry Pi 2 ajánlott.
A megvizsgált HWRNG-k nem biztosítanak megnyugtató entrópiát, de a legkevesebb problémát a Raspberry PI esetében találtuk.
Az azonos SoC-okra épülő SBC-k eltérő memóriasebessége nem befolyásolja jelentős mértékben az SBC teljesítményét.

Összefoglalás és további kutatások

A vizsgálatok alapján az SBC-k költséghatékony, energiatakarékos, az információbiztonság területén jól alkalmazható eszközök.
A felhasználási lehetőségek meghatározására újabb, a titkosítási képességeket vizsgáló mérések kidolgozása és elvégzése szükséges (Pl: HTTPS, SCP, SFTP, IPSec). Nagyon fontos vizsgálandó terület a hálózati átviteleknél produkált teljesítmény. Mérések kidolgozása és elvégzése szükséges a biztonsági alkalmazások során tanúsított teljesítményre vonatkozóan (pl: valós idejű forgalomanalízis (IDS), tűzfal, mintakeresés, Hadoop).
Végül fontos az egyes SBC-k virtualizációs képességeinek, valamint, más, biztonsági területen elterjedt operációs rendszerekkel való kompatibilitásának a vizsgálata. (Pl: OpenBSD, FreeBSD.)

Köszönet

Köszönjük a HunNet-Média Kft-nek, hogy a vizsgálatokhoz rendelkezésünkre bocsátotta az egykártyás számítógépeket, ezáltal is hozzájárulva a publikáció létrejöttéhez.

Referenciák

[1] http://www.arm.com
[2] https://www.raspberrypi.org
[3] ODROID-XU3 Lite, http://www.hardkernel.com/main/products/prdt_info.php?g_code=G141351880955
[4] Habibah Hashim et al: A Series of Secret Keys in a Key Distribution Protocol, London, UK, 2014. július 2-4, Springer, 615-628.
[5] BeagleBone Black, http://beagleboard.org/black
[6] LMbench, http://lmbench.sourceforge.net/
[7] Carel Kruger és Gerhard Hancke: Benchmarking Internet of things devices, Porto Alegre, Brazília, 2014. július 27-30, IEEE, 611-616.
[8] Robert Graham Reed et al: A CPU benchmarking characterization of ARM based processors, Moszkva, Oroszország, 2015, Lomonosov Moscow State University, 581-586.
[9] George Thomas Wrigley et al: Memory benchmarking characterisation of ARM-based SoCs, Moszkva, Oroszország, 2015, Lomonosov Moscow State University, 607-613.
[10] Intel Atom processor, http://www.intel.com/content/www/us/en/processors/atom/atom-processor.html
[11] http://pandaboard.org/
[12] Edson L. Padoin et al: Evaluating Performance and Energy on ARM-based Clusters for High Performance Computing, Pittsburgh, USA, 2012. szeptember 10-13, IEEE, 165-172.
[13] Lencse Gábor és Répás Sándor: Method for Benchmarking Single Board Computers for Building a Mini Supercomputer for Simulation of Telecommunication Systems, Prága, Csehország, 2015. július 9-11, Brno University of Technology, 246-251.

[14] Lencse Gábor, Derka István és Muka László: Towards the Efficient Simulation of Telecommunication Systems in Heterogeneous Distributed Execution Environments, Róma, Olaszország, 2013. július 2-7, Brno University of Technology, 304-310.
[14] Announcing the ADVANCED ENCRYPTION STANDARD (AES), USA, 2001. november 26, National Institute of Standards and Technology
[15] Nagy, I. Z.: Spezielle Eintreibungstechniken zur Senkung der Außenstände, In: Kadocsa Gy (szerk.), MEB 2006: 4th International Conference on Management, Enterprise and Benchmarking. 360 p., Budapest BMF.,2006. pp. 196-208., (ISBN: 9637154477)
[16] Nagy, I. Z., Való, V.: The Lawful Execution of Employer's Rights is an Important Subsystem of Corporate Governance: a Labour Case Study, In: Michelberger, P. (szerk.), MEB 2013: 11th International Conference on Management, Enterprise and Benchmarking: Budapest: Óbudai Egyetem, 2013. pp. 107-126. (ISBN: 978-615-5018-58-9)