aselsan

www.aselsan.com.tr

ASELSAN Türk Silahlı Kuvvetlerini Güçlendirme Vakfı'nın bir kuruluşudur.

SIRASIZ İŞLEMCİLER İÇİN ÖZEL AES BUYRUKLARI EKLEME

Gökhan KAPLAYAN

ITC-2019

AJANDA

aselsan

- Giriş/Ön Bilgi
- Mimari Detayları
- Test Ortamı
- Sonuç ve Değerlendirmeler

Gözlem

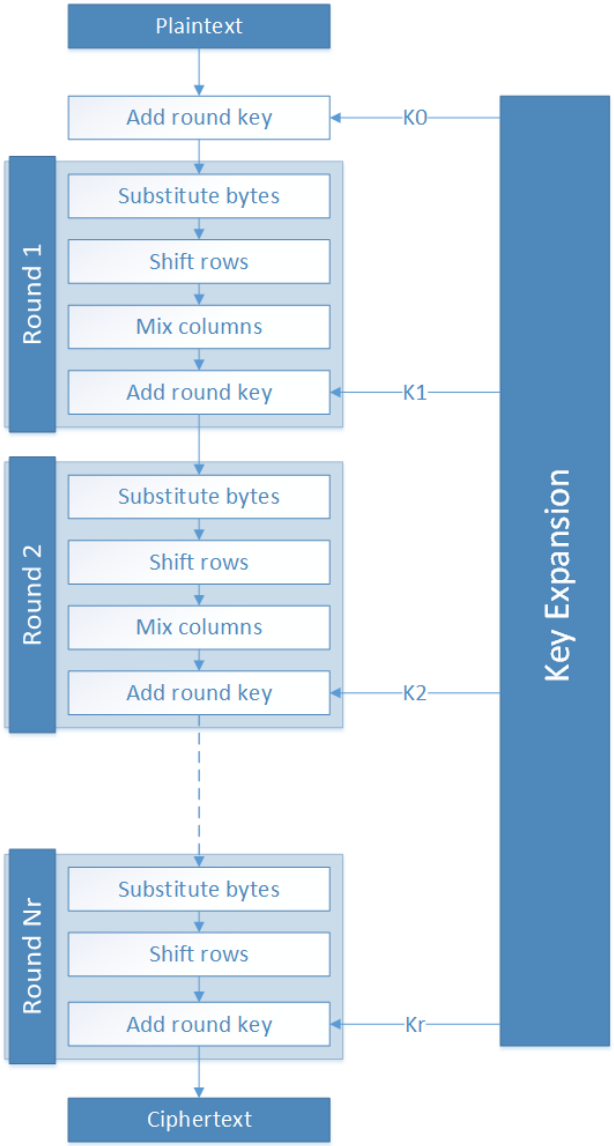
- AES algoritması kriptolojide en çok kullanılan algoritmalardan biri
- Yüksek performanslı ve güvenlikli şifreleme ihtiyacı

AES algoritması gerçekleme yöntemleri:

Gerçekleme Yöntemi	Performans	Esneklik
Genel amaçlı buyruklar ile yazılım	✗	✓
Özel donanım	✓	✗
Özel donanım + Özel buyruklar ile yazılım	✓	✓

AES ALGORİTMASI

aselsan



AES algoritması ‘round’lardan oluşur:

- Substitute bytes
- Shift rows
- Mix columns
- Add round key

Anahtar Uzunluğu	Round Sayısı
128-bit	10+1
192-bit	12+1
256-bit	14+1

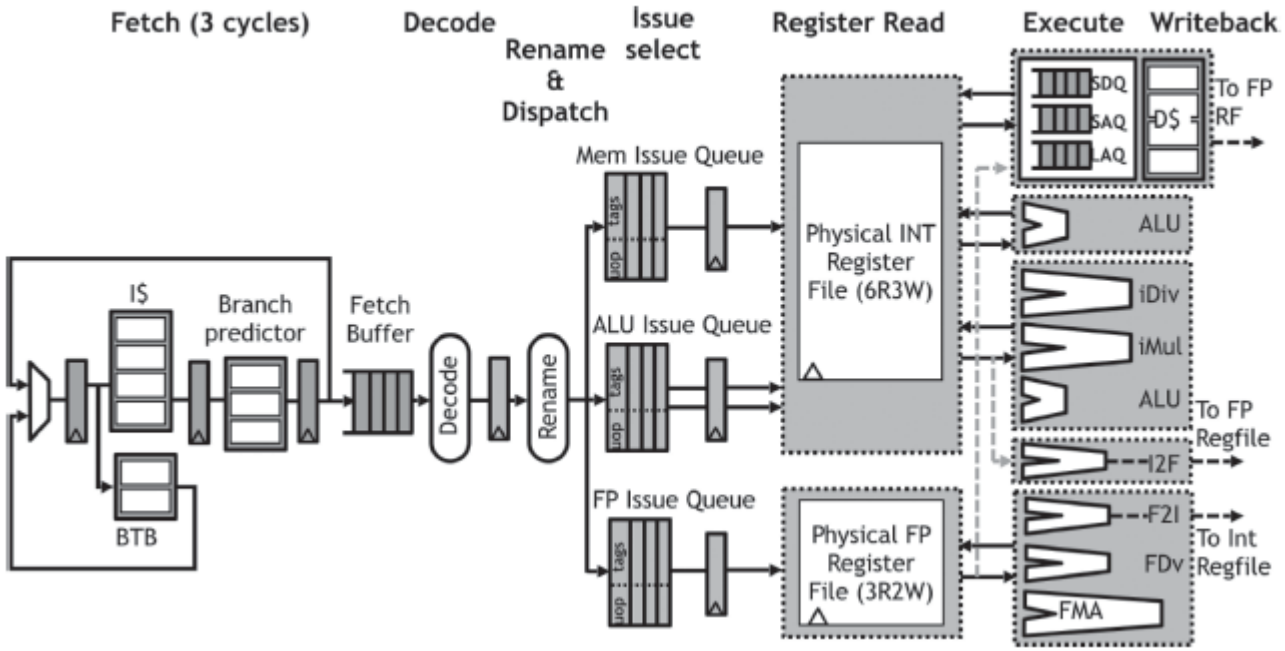
ÖZEL AES BUYRUKLARI

aselsan

Buyruk	Yazmaç	Tanım
aeskey	rs1,rs2	Türetilmiş anahtarları yükleme
aesend	rs1,rs2	Son türetilmiş anahtarı yükleme
aesenc	rd,rs1,rs2	128-bit blok şifreleme ve 64-bit sonucu yükleme
aesdec	rd,rs1,rs2	128-bit blok şifre çözme ve 64-bit sonucu yükleme
aesload	rd	Şifreleme işlemi sonucu kalan 64-bit sonucu yükleme

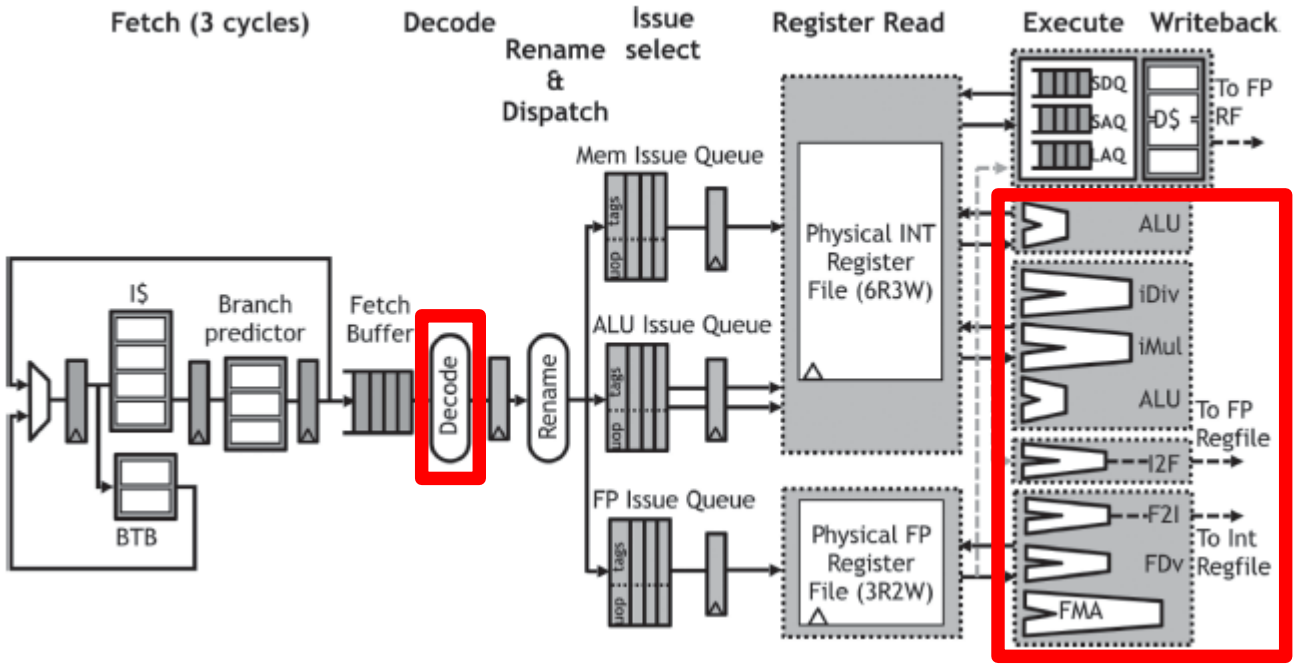
RISC-V ISA genişlemesi

- Derleyici
- İşlemci Mimarisi



64-bit RISC-V İşlemci Çekirdeği:

- Sırasız Yürütme
- Çoklu İşleme
- Spekülatif İşlemler

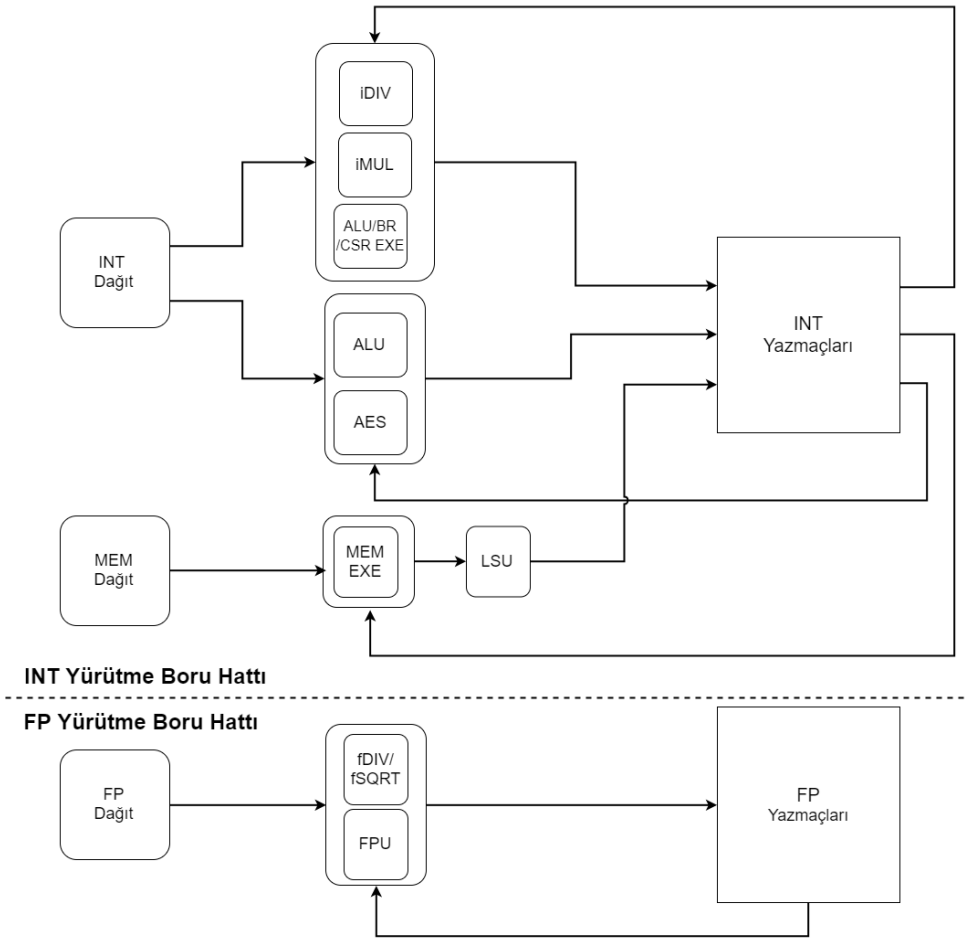


- Çöz
  - Özel AES buyrukları tanımı
- Yürütme
  - AES modülünü ekleme

YÜRÜTME

aselsan

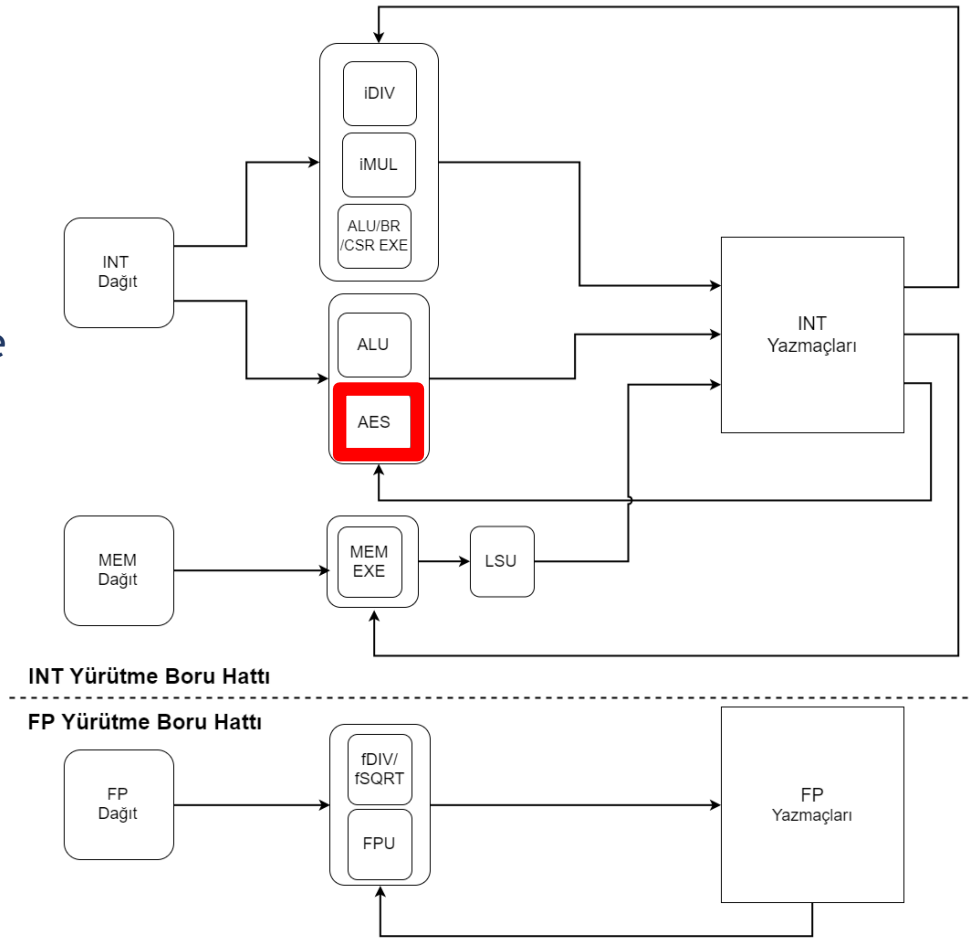
Buyruk Tipleri	Fonksiyonel Modüller
Tam Sayı Aritmetik	ALU
Dallanma	BRU
Hafıza Erişimi	MEM EXE + LSU
Tam Sayı Bölme	iDIV
Tam Sayı Çarpma	iMUL
CSR Kontrol	CSR EXE
Kayan Nokta Aritmetik	FPU
Kayan Nokta Bölme	fDIV/fSQRT
AES İşlemleri	AES



YÜRÜTME

aselsan

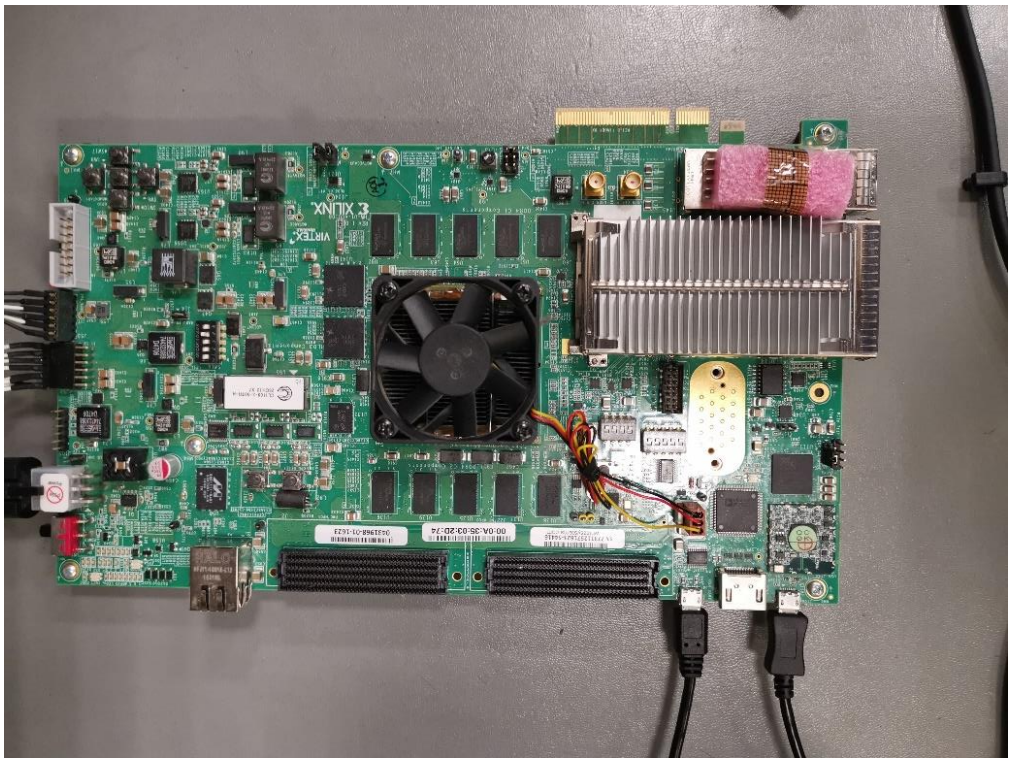
- Tek Yazmaç Yazma Portu
  - İki buyruk ile sonuç yükleme
- Port Paylaşımı
  - Dağıt portu
  - Yazmaç portları
- Gerçekleme Zorlukları
  - ‘Routing congestion’



PERFORMANS DEĞERLENDİRMESİ

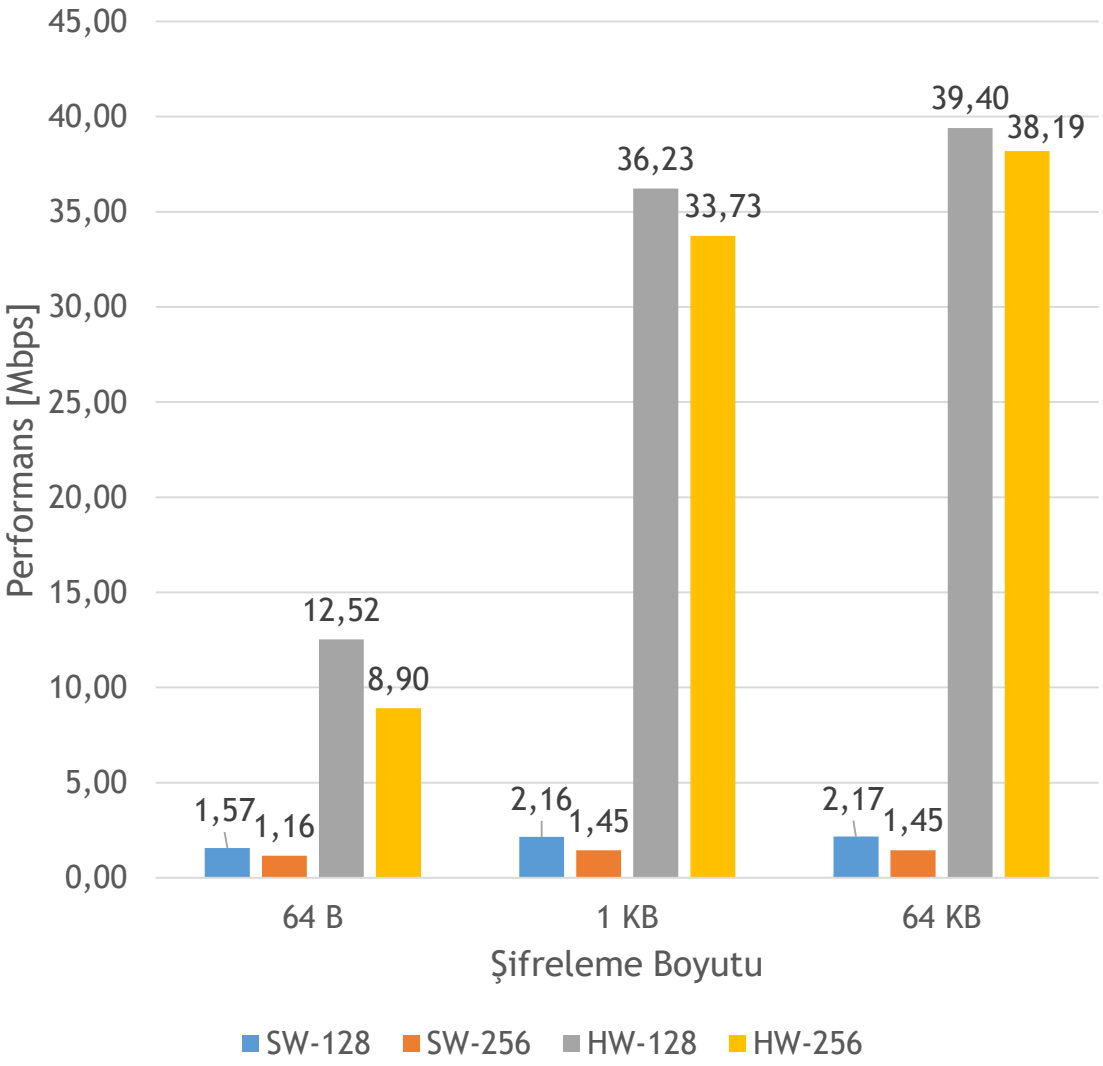
aselsan

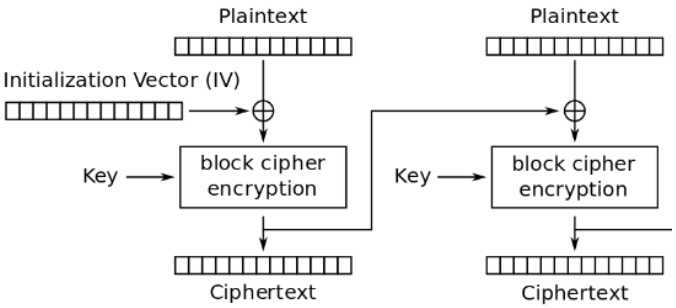
- Açık kaynak AES yazılımı
  - Özel buyrukları ‘inline assembly’ kodu ile kullanmak
- Test ortamı
  - FPGA kartı: Xilinx VCU108
  - Saat frekansı: 50 MHz



AES CBC

aselsan





AES CBC Blok Şeması

KARŞILAŞTIRMA

aselsan

İşlemciler	Saat Frekansı [MHz]	SW Performansı [MB/s]	HW Performansı [MB/s]	HW Performansı [KB/(s*MHz*Core)]
BOOM-AES	50	0.27	4.92	**100.76**
ESP32*	240	1.10	5.28	22.52
PIC32MZ*	200	0.26	5.78	29.59
STM32F756*	216	3.38	15.02	6.79
Apple A11 (6 core)*	2.39 [GHz]	24.94	912.34	63.62

Karşılaştırma Parametreleri:

- Mod: AES-CBC-128
- Şifreleme boyutu: 64 KB

*Performans sonuçları şu siteden alınmıştır: wolfssl.com/docs/benchmarks/

KAYNAK KULLANIMI ve ZAMANLAMA

aselsan

- Kaynak Kullanımı

	LUTs	FFs	RAMB36
Çekirdeğin toplam kaynak kullanımı	186.667	61581	17
AES modülünün kaynak kullanımı	601 (%0.3)	585 (%0.9)	10 (%58)

- Zamanlama Etkisi

	Positive Slack
Bütün tasarımın en kötü zamanlaması	+1.022 ns
AES modülü ile ilgili en kötü zamanlama	+5.667 ns

SONUÇ

aselsan

- RISC-V ISA genişlemesi
- Sırasız işlemci için AES modülü eklenmesi
  - AES algoritması için ~25x performans
- Yapılacak çalışmalar
  - Detaylı doğrulama çalışması
  - Sırasız ve spekülatif AES buyrukları yürütme
  - ASIC tasarım süreci için değerlendirme

TEŞEKKÜRLER ☺

Referanslar

aselsan

1. Daemen, Joan, and Vincent Rijmen. "AES proposal: Rijndael." (1999).
2. Chen, Lily, et al. Report on post-quantum cryptography. US Department of Commerce, National Institute of Standards and Technology, 2016.
3. R. B. Lee, Z. Shi, and X. Yang. Efficient permutation instructions for fast software cryptography. IEEE Micro, 21(6):56-69, Nov./Dec. 2001.
4. Brickell, Ernie, et al. "Software mitigations to hedge AES against cache-based software side channel vulnerabilities." IACR Cryptology ePrint Archive 2006 (2006): 52.
5. Akdemir, Kahraman, et al. "Breakthrough AES performance with intel AES new instructions." White paper, June (2010): 11.
6. Bertoni, Guido Marco, et al. "Speeding up AES by extending a 32 bit processor instruction set." IEEE 17th International Conference on Application-specific Systems, Architectures and Processors (ASAP'06). IEEE, 2006.
7. Elbirt, Adam J. "Fast and efficient implementation of AES via instruction set extensions." 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07). Vol. 1. IEEE, 2007.
8. Tillich, Stefan, Johann Großschädl, and Alexander Szekely. "An instruction set extension for fast and memory-efficient AES implementation." IFIP International Conference on Communications and Multimedia Security. Springer, Berlin, Heidelberg, 2005.
9. Webb, Charles F. "IBM z10: The next-generation mainframe microprocessor." IEEE micro 28.2 (2008): 19-29.
10. C. Celio, P.-F. Chiu, B. Nikolic, D. A. Patterson, and K. Asanovi,“Boom v2: an open-source out-of-order risc-v core,” tech. rep., EECS Department, University of California, Berkeley, 2017.
11. Waterman, Andrew, et al. "The risc-v instruction set manual, volume i: Base user-level isa." EECS Department, UC Berkeley, Tech. Rep. UCB/EECS-2011-62 116 (2011).
12. J. Bachrach, H. Vo, B. Richards, Y. Lee, A. Waterman, R. Avi˘zienis, J. Wawrzynek, and K. Asanovi´c, “Chisel: Constructing hardware in a scala embedded language,” in DAC Design Automation Conference 2012,June 2012, pp. 1212–1221.
13. https://github.com/riscv/riscv-gcc
14. https://github.com/hplp/aes_chisel
15. https://github.com/kokke/tiny-AES-c
16. https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

AES-128 Anahtar Yükleme

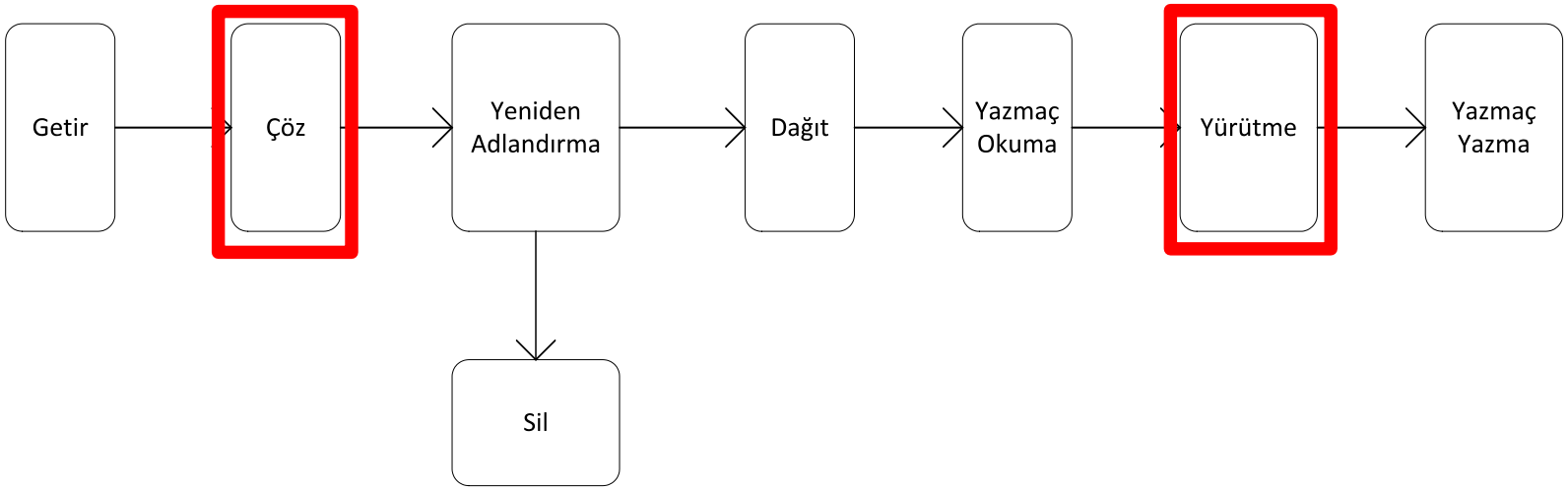
```
uint64_t c; //dummy value
uint64_t **key_64;
*key_64 = RoundKey; // for casting from 8-bit to 64-bit
asm volatile("aeskey %[z], %[x], %[y]\n\t": [z] "=r" (c) : [x] "r" (((*key_64)[0])), [y] "r" (((*key_64)[1])));
asm volatile("aeskey %[z], %[x], %[y]\n\t": [z] "=r" (c) : [x] "r" (((*key_64)[2])), [y] "r" (((*key_64)[3])));
……
asm volatile("aeskey %[z], %[x], %[y]\n\t": [z] "=r" (c) : [x] "r" (((*key_64)[18])), [y] "r" (((*key_64)[19])));
asm volatile("aesend %[z], %[x], %[y]\n\t": [z] "=r" (c) : [x] "r" (((*key_64)[20])), [y] "r" (((*key_64)[21])));
```

AES Şifreleme

```
uint64_t **buf_64;
*buf_64 = buf; // for casting from 8-bit to 64-bit
asm volatile("aesenc %[z], %[x], %[y]\n\t": [z] "=r" (((*buf_64)[0])) : [x] "r" (((*buf_64)[0])), [y] "r" (((*buf_64)[1])));
asm volatile("aesload %[z], %[x], %[y]\n\t": [z] "=r" (((*buf_64)[1])) : [x] "r" (((*buf_64)[0])), [y] "r" (((*buf_64)[1])));
```

Mimari

aselsan



- Çöz
  - Özel AES buyrukları tanımı
- Yürütme
  - AES modülünü ekleme

BENZER ÇALIŞMALAR

aselsan

ISA Genişlemesi

- AES ‘round’u için buyruk
  - Intel ve AMD (AES-NI)
  - ARM
- AES algoritması için buyruk
  - IBM

‘Memory-mapped’ Hızlandırıcı

- STM32
- Infineon AURIX
- Atmel XMEGA

ÇÖZ

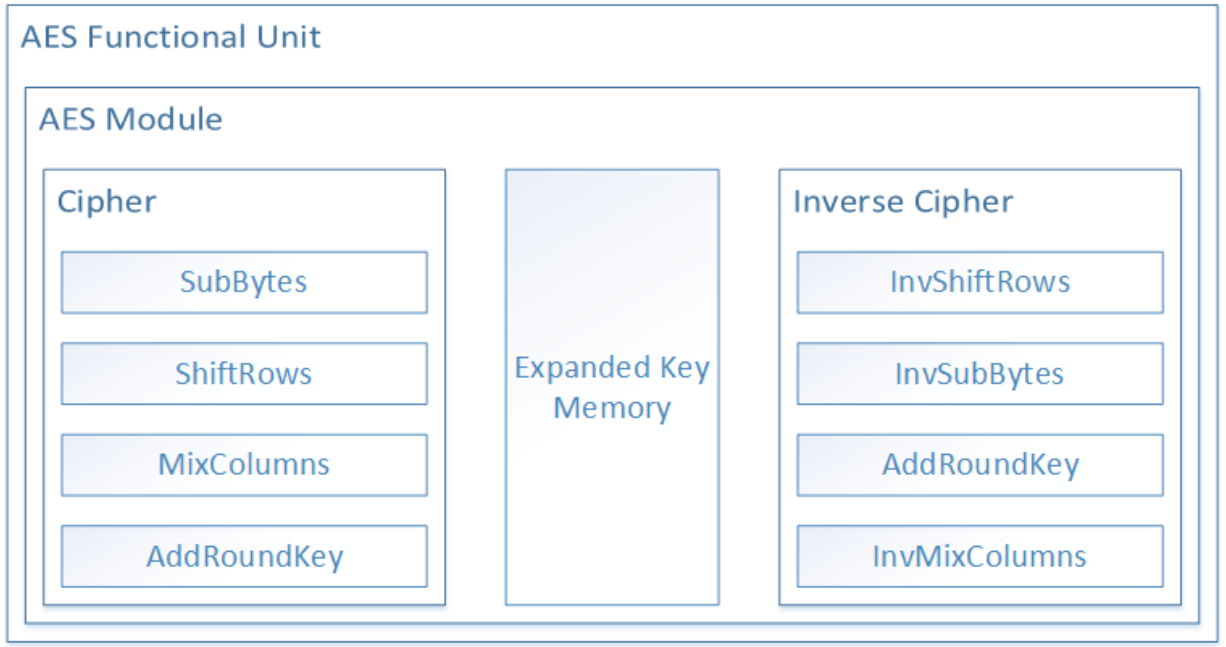
aselsan

Beklenen Buyruk Davranışı	AES Buyrukları Davranışı	Çöz Biriminde Çözüm

• Yazmaca yazma
• Yan-kanal etkisi bırakmama
	• Sıralı anahtar yükleme
	• İki buyruk ile sonuç yükleme
	• **Yan-kanal etkisi!**
		• AES buyruklarını
		  • Sıralı ve
		  • Spekülasyon olmadan yürütme

AES MODÜLÜ

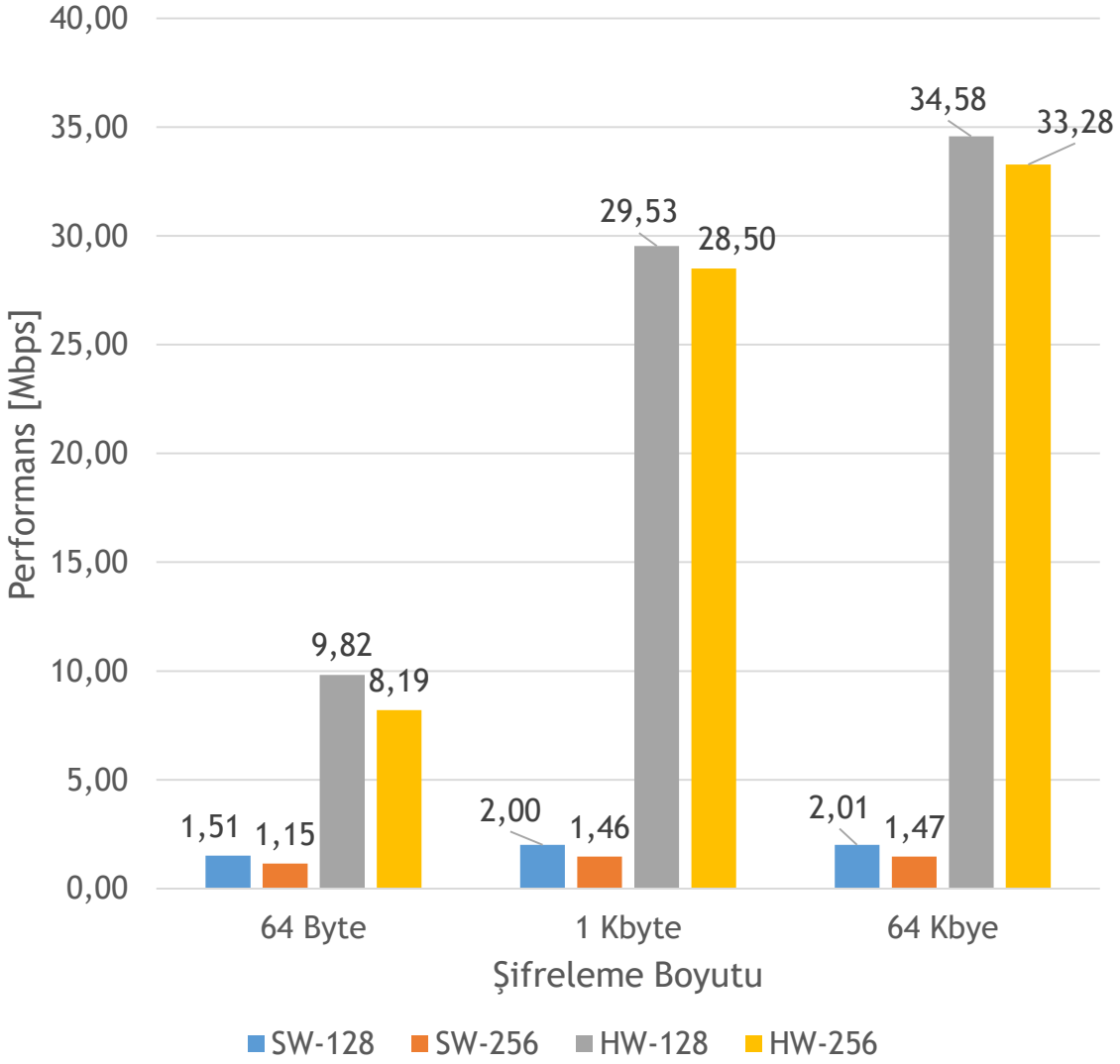
aselsan

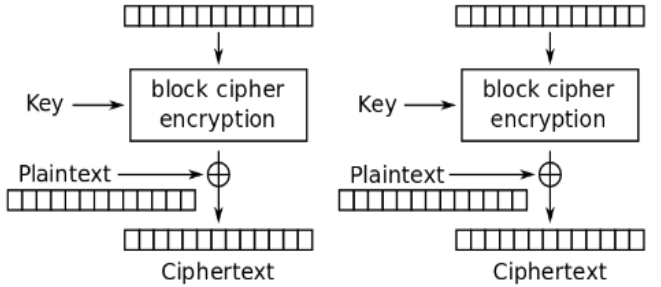


- AES Modülü
  - Türetilmiş Anahtar Hafızası
  - Şifreleme
  - Şifre Çözme
- AES Fonksiyonel Modülü
  - ‘Iterative’

AES CTR

aselsan





AES CTR Blok Şeması