UNIVERSITY OF PASSAU

Faculty of Computer Science and Mathematics

Kriptografik Algoritmaların Donanım Üzerinde Fiziksel Saldırılara Karşı Güvenli Gerçeklenmesi

Elif Bilge Kavun

5 Mayıs 2023

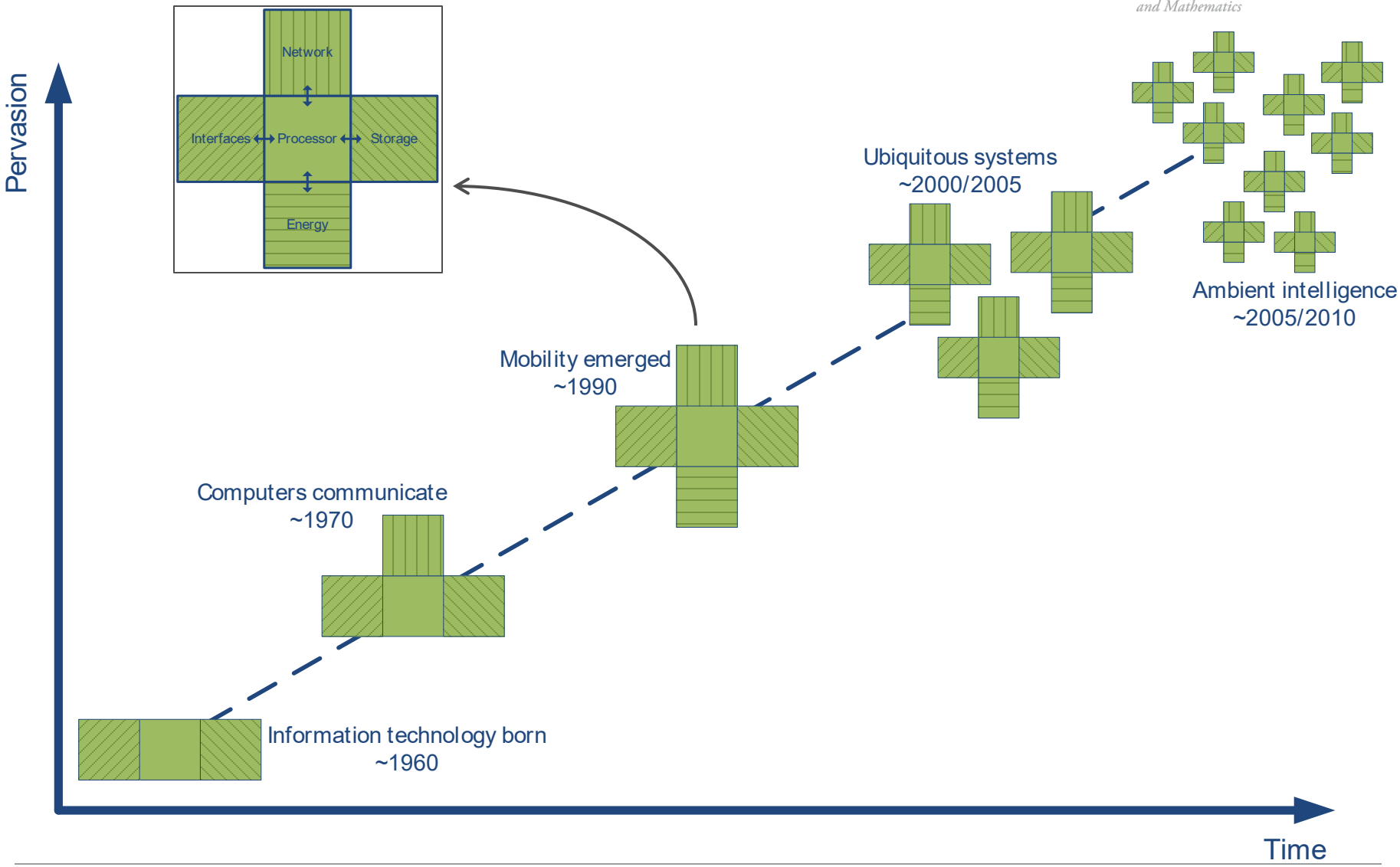
Ben Kimim?

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

- BScEE (İYTE)
- MSc Kriptografi (ODTÜ)
- Doktora: Bochum Ruhr Üniversitesi (Almanya), Gömülü Güvenlik
  - Tez "Kaynak kısıtlı (hafif) kriptografi"
- Altı yıllık endüstri ve danışmanlık deneyimi
  - Farklı şirketlerin donanım güvenliği projelerinde staj ve danışmanlık (Türkiye, ABD)
  - Sayısal Tasarım Mühendisi - Kripto Blokların Güvenli Tasarımı, Infineon (Almanya)
  - Siber Güvenlik alanında Doktor Öğretim Üyesi, Sheffield Üniversitesi (Birleşik Krallık)
- Ekim 2020'den beri
  - Güvenli Akıllı Sistemler alanında Doktor Öğretim Üyesi, Passau Üniversitesi (Almanya)
- Ana çalışma alanları/araştırma ilgi alanları
  - Donanım güvenliği
  - Kriptografik şemaların tasarımı ve uygulanması
  - Hafif kriptografi
  - Yan kanal saldırıları ve karşı önlemler
  - Akıllı sistemlerin güvenliği
  - Güvenlik uygulamaları için yapay zeka

- Kriptografik Yapılar
- Kriptografik Algoritmaların Gerçeklenmesi
  - Ölçütler
  - Yazılım / Donanım
- Fiziksel Saldırılar
  - Karşı Önlem Mekanizmaları
  - Rastgele Sayı Üretimi İhtiyacı

Bilişim Çağı



Nesnelerin İnterneti ve Uygulamalar

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

Akıllı evler

Akıllı telefonlar
Mobil uygulamalar

Otomasyon bileşenleri
Demirbaş takip sistemleri

Ödeme ve ücret toplama kartları

Elektronik pasaportlar

Otomobil anahtar sistemleri

Dayanıklı Güvenlik Mimarileri İhtiyacı

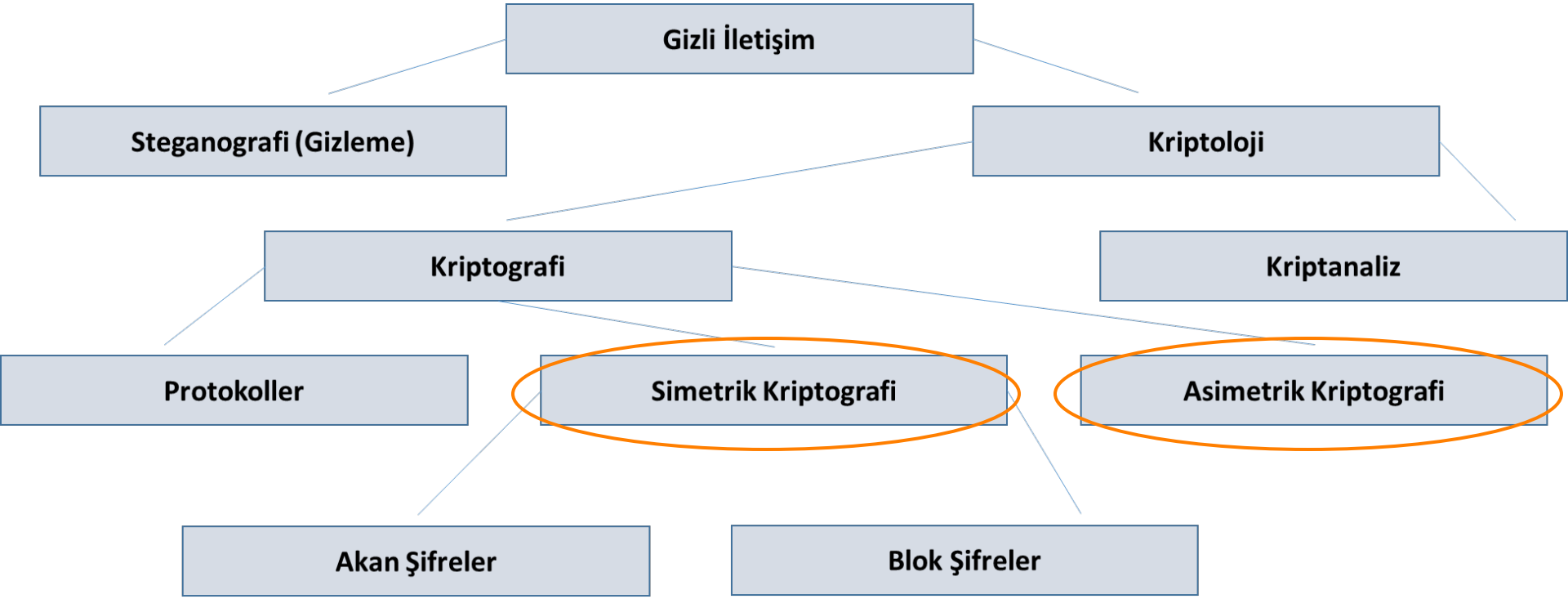
UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

- Erişim kontrolü
- Veri gizliliği
- Bilgi güvenliği
- Sahteciliğin azaltılması
- Kişisel verilerin gizliliği ve korunması (mahremiyet)

Bilgi Güvenliği ve Fiziksel Saldırılar

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

Kriptografik Yapılar: Terminoloji



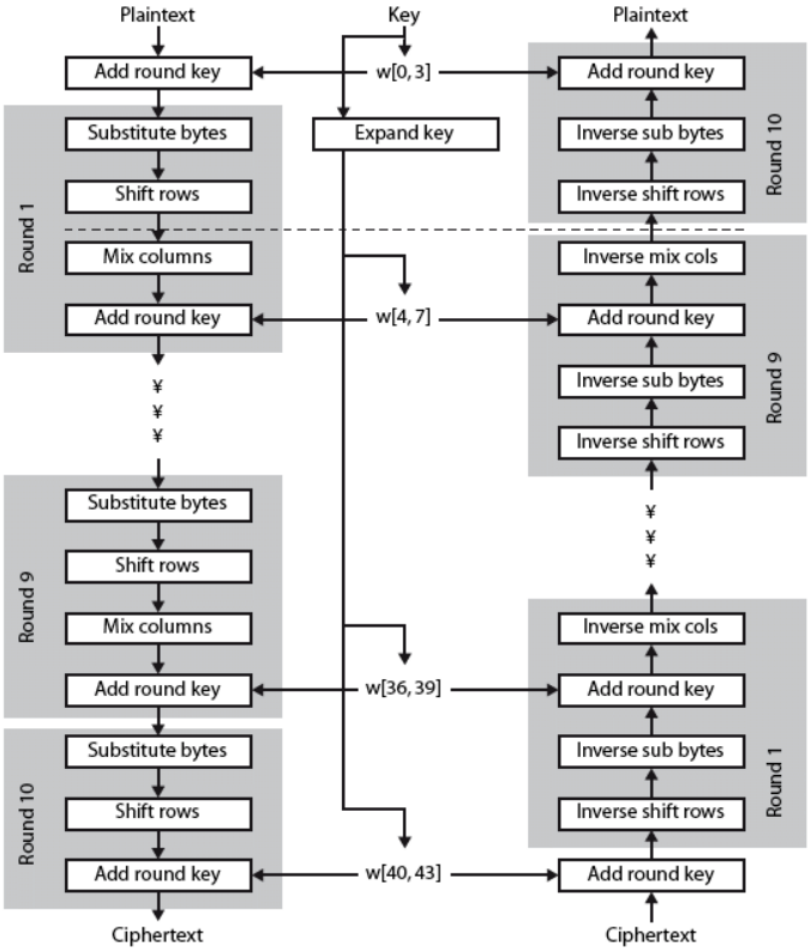
- Simetrik
  - Gizli anahtarlı
  - Avantaj: Daha kısa anahtar, daha hızlı işlem
  - Dezavantaj: Tek ve aynı anahtar, anahtar güvenliği
  - Kullanım: Genelde hareket halinde olmayan veriler

- Asimetrik
  - Gizli ve açık anahtarlı
  - Avantaj: Gizli anahtar, anahtar paylaşılmaması
  - Dezavantaj: Uzun işlem süreleri
  - Kullanım: Güvenli ödeme, işlem yetkilendirme, dijital sertifikalar

- Düz metin simetrik şifreleme kullanılarak şifrelenir
  - Daha hızlı işlem

- Asimetrik şifreleme, simetrik şifreleme için kullanılan anahtar değişimi için kullanılır
  - Anahtara yalnızca hedeflenen alıcı ulaşabilir
  - Örnekler:
    - SSL/TLS bağlantıları
    - Uçtan uca şifreleme kullanan Signal, WhatsApp gibi mesajlaşma uygulamaları

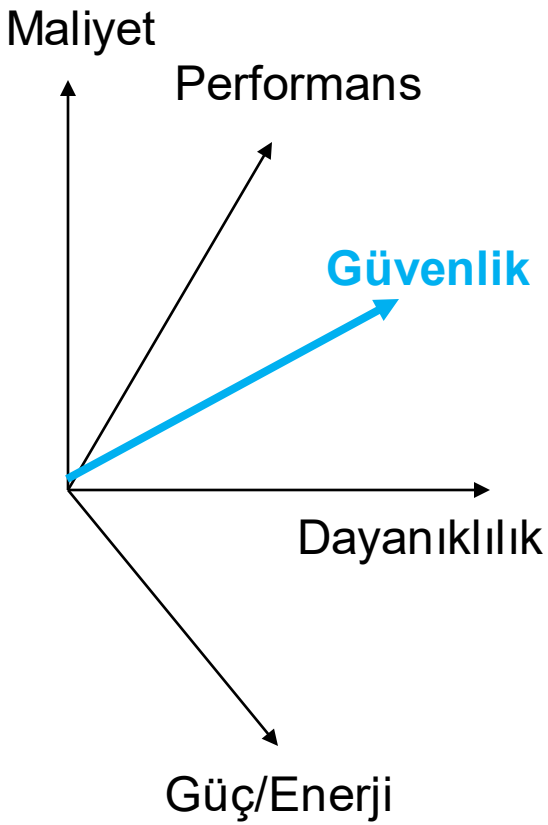
UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics



- **Standart algoritmalar**
  - Sunucular, güçlü bilgisayar ve mobil cihazlar
  - **Simetrik:** AES, DES
  - **Asimetrik:** RSA
- **Hafif algoritmalar**
  - Nesnelerin interneti, gömülü sistemler
  - **Simetrik:** PRESENT, CLEFIA, …
  - **Asimetrik:** ECC

- Özet fonksiyonlar
- Kuantum sonrası kripto

Tasarım Ölçütleri

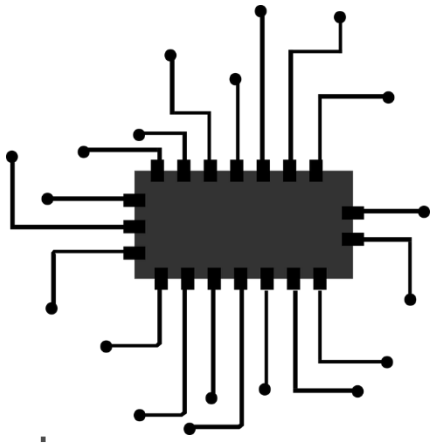


- Bir sistem veya bir bileşen, belirli bir işlevselliği gerçekleştirmek üzere tasarlanır
- Her tasarım seçimi, alan veya gecikme süresi gibi özelliklerle ilişkilidir
- Global kararlar (örn. ASIC veya FPGA veya yazılım) ve yerel optimizasyonlar tasarım uzayında farklı noktaları işaret eder

Tasarım Ölçütleri

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

- Tasarımda genel olarak şu ölçütler hedeflenir
  - Maliyet
  - Performans
  - Güç/Enerji Tüketimi
  - Dayanıklılık



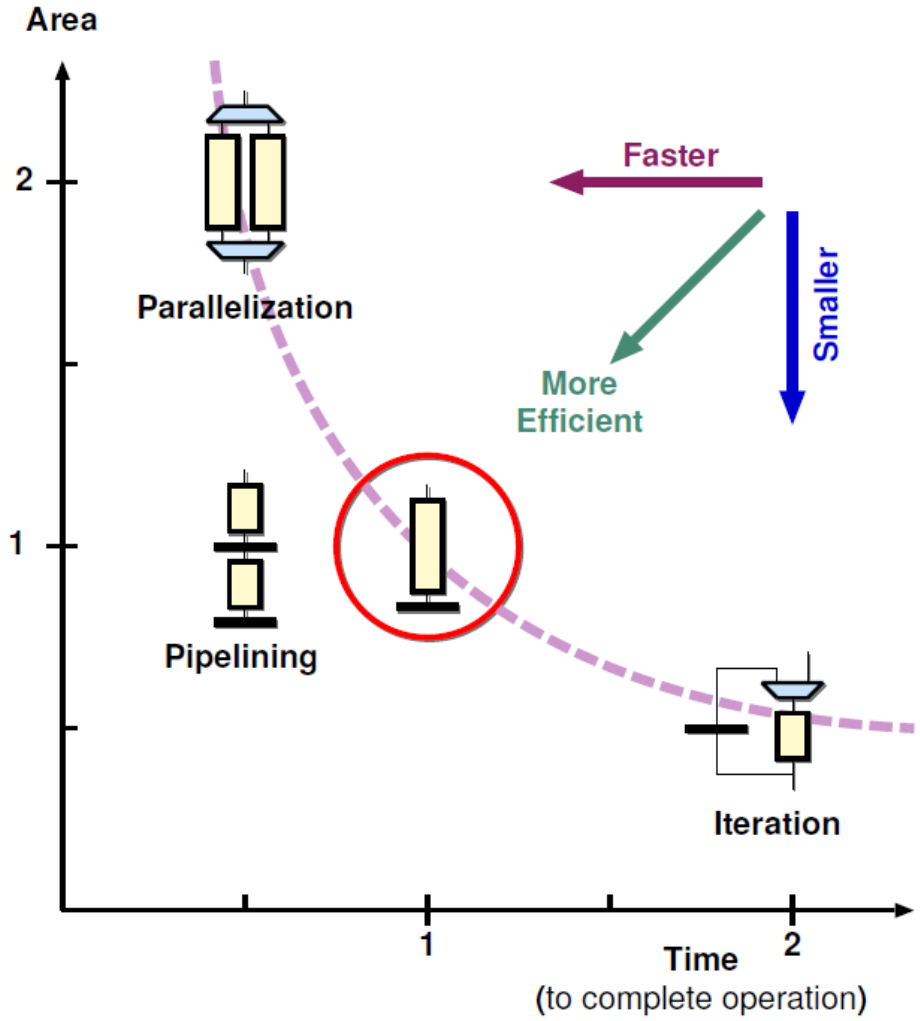
- Bunlar, birbirleriyle çelişebilecek belirli hedefler içerir
- Tasarım seçimleri belirli hedefleri iyileştirirken diğerlerini kötüleştirebilir
- Odak noktamız: Bu hedeflerin **güvenlik**le olan ilişkisi

Tasarım Ölçütleri – Hedefler

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

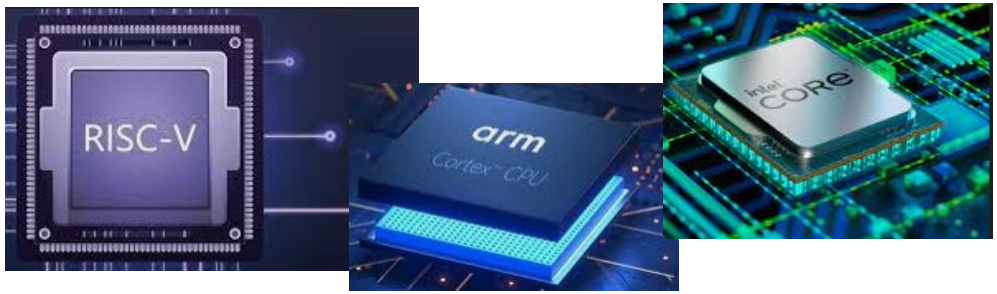
- Yüksek Hız
  - Bazı uygulamalar için oldukça yüksek hız (bulut bilişim, özet fonksiyonları, vs.)
  - Genelde orta hızları: 1 Mbit/s - 100 Mbit/s
  - Kaynak kısıtlı uygulamalarda daha da az olabilir
- Düşük Gecikme Süresi
  - Kimlik doğrulama, insan etkileşimi: <100 ms
- Düşük Alan
  - Maliyet sorunu
  - Ekstra özelliklerle artar: spesifik güvenlik ihtiyaçları
- Düşük Güç
  - Pasif RFID destekli sistemler, pik güç sorunları
- Düşük Enerji
  - Mobil/pille çalışan sistemler, bilgi işlem çiftlikleri

Tasarım Ölçütleri – Hedefler

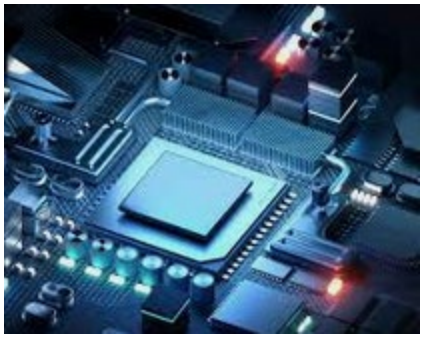


Kriptografik devre optimizasyonları

- Gömülü cihazlar üzerindeki uygulamalar için: *Yazılım* odaklı çözümler
  - Pazara sunma süresi
  - Geliştirici sayısı



- Bazı durumlarda daha iyi performans için: *Donanım*
  - Kripto gibi karmaşık işlemleri hızlandırma amaçlı
  - GPU da mümkün, ama her zaman yeterli olmayabilir



- Donanım/yazılım ortak tasarımları

- Komut seti uzantıları (ISE)
  - Intel AES-NI
  - Açık kaynaklı RISC-V işlemcisini hedefleyen

- Donanım uygulamaları
  - Kriptografi tasarımları/problemleri için donanım hızlandırma
  - Uygulamaya Özel Entegre Devrelerin (ASIC) Hedeflenmesi
  - Sahada Programlanabilir Kapı Dizilerinin (FPGA) Hedeflenmesi
  - Farklı tasarım yaklaşımları: Paralel, seri, açılmış algoritma

Donanım/Yazılım Ortak Tasarımı

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

- Donanım hızlandırıcısı yazılımı destekler
- Yazılımda karmaşık kriptografik işlemler gerçekleşeceği zaman donanım hızlandırıcısını çağırır
- Toolchain desteği şart değil
  - Yeni komutlar eklemek için derleyiciyi vs. değiştirme ihtiyacı yok

Lightweight and Reconfigurable IPSec Core [1]

UNIVERSITY OF PASSAU
Faculty of Computer Science

IPSECCO: A Lightweight and Reconfigurable IPSec Core

Benedikt Driessen, Tim Güneysu, Elif Bilge Kavun, Oliver Mischke, Christof Paar, Thomas Pöppelmann
Horst Görtz Institute for IT-Security
Ruhr-University Bochum, Germany
{benedikt.driessen, tim.gueneysu, elif.kavun, oliver.mischke, christof.paar, thomas.poeppelmann}@rub.de

***Abstract*—In this paper we propose a reconfigurable lightweight Internet Protocol Security (IPSec) hardware core. Our architecture supports the main IPSec protocols; namely Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE). In this work, the cryptographic algorithms and their modes of operation, which are at the heart of the IPSec protocols, are implemented in hardware. Instead of re-implementing common IPSec configurations, which are deemed "too heavy" for pervasive devices, we evaluate efficient implementations of standardized and/or well-known lightweight and hardware-friendly algorithms. In particular, we examine different versions of PRESENT, GRØSTL, PHOTON, and a very compact ECC core. As a consequence, we present IPSECCO, a core with adequate security and only moderate resource requirements, making it suitable for lightweight devices. We selected the Xilinx Spartan family of Field Programmable Gate Arrays (FPGA) as target platform due its low-power footprint and reduced costs compared to other FPGAs. Our results show that it is possible to realize a high performance IPSec core even on members of the Spartan-3 family.**

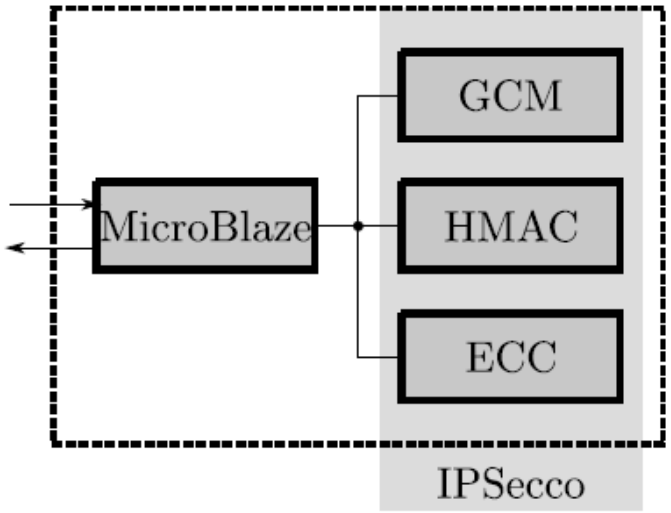
***Keywords*-Lightweight; IPSec; FPGA; Reconfigurability**

attempts to the data transmission, data integrity – to make sure that the transferred data is not changed, and authentication – to identify the information source. In IPSec, there are different protocols to provide mentioned services. For instance, the Authentication Header (AH) protocol provides data authentication. The Encapsulating Security Payload (ESP) protocol defines mechanisms for confidentiality and data integrity. Finally, the Internet Key Exchange (IKE) protocol is used for establishing secure connections. These protocols use different cryptographic primitives such as encryption, hashing and modular arithmetic in order to provide security services. A minimum set of algorithms, which must be supported in an IPSec implementation for AH, ESP, and IKE protocols, was defined in "Cryptographic Suites for IPSec" [6], [7] for standardization purposes. For example, in "Cryptographic Suite B" [7], the AES [8] cipher is used in Galois/Counter Mode (GCM) [9] to provide authenticated encryption. The Hashed Message Authentication Code (HMAC) [10] con-

[1] Driessen et al (2012). "IPSecco: A Lightweight and Reconfigurable IPSec Core". IEEE ReConFig Conference.

Lightweight and Reconfigurable IPSec Core [1]

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics



	AH (HMAC)	ESP (GCM)	IKE
IPSECCO-80	PHOTON	PRESENT-80 (B)	ECC (secp160r1)
IPSECCO-128	GRØSTL	PRESENT-128 (S)	ECC (secp256r1)

- İşlemci mimarisine kripto gibi karmaşık işlemler için yeni komutlar eklenir
  - Sistem performansına katkı

- Sadece donanım değişiklikleri değil, aynı zamanda toolchain (derleyici vb.) desteği de gereklidir

- Örnek: Intel AES-NI ISE

Intel's AES Instruction Set Extension [2]

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

Komut	Tanım
AESENC	AES şifreleme algoritmasının bir round'u
AESENCLAST	AES şifreleme algoritmasının son round'u
AESDEC	AES deşifreleme algoritmasının bir round'u
AESDECLAST	AES deşifreleme algoritmasının son round'u
AESKEYGENASSIST	AES round anahtarı üretimi desteği
AESIMC	AES Inverse MixColumns desteği
PCLMULQDQ	GF(2)'de Carryless Çarpım

[2] Shay Gueron (2010). "Intel Advanced Encryption Standard (AES) Instruction Set White Paper". Intel.

- Farklı hedef platformlar
  - ASIC'ler
  - FPGA’lar

- FPGA’lerin ASIC’lere üstünlüğü
  - Yeniden yapılandırılabilirlik
  - Gerçekçi değerlendirmeler için pratik
  - Ticari kullanımda düzeltmesi/güncellemesi daha kolay

- Kaynaklar her zaman birebir eşleşmeyebilir
  - **Kapılar veya Kapı Eşdeğerleri** vs. **DSP ve RAM Blokları, slice'lar**

Table 1. Comparison of Different S-boxes [3]

Implementation Platform	PRESENT[6]	MIBS[28]	LBlock[39]	Piccolo[27]
ASIC (GE)	28	24	22	12
FPGA (SLICE)	2	2	2	2

[3] Kolay and Mukhopadhyay, Khudra: A New Lightweight Block Cipher for FPGAs, SPACE'14, 2014.

- Farklı tasarım yaklaşımları
  - Paralel
  - Pipelined
  - Seri
  - Açılmış algoritma

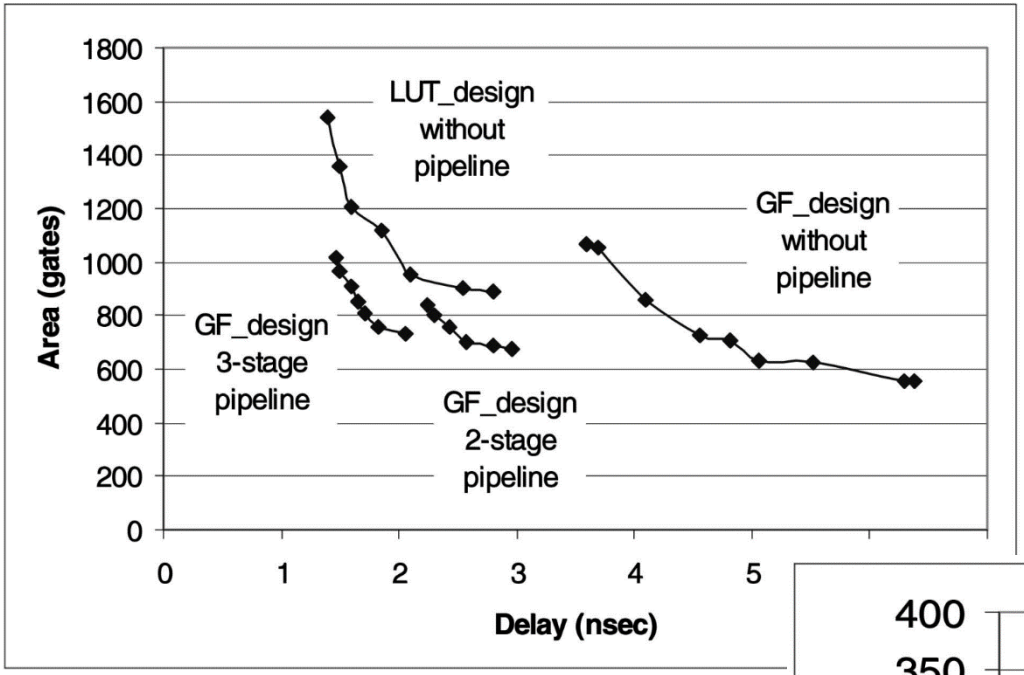
- Farklı tasarım hedefleri
  - Düşük alan kullanımı
  - Düşük enerji kullanımı
  - Düşük güç kullanımı
  - Yanıt gecikmesi olabildiğince kısa

- Bileşen düzeyinde optimizasyon
  - İşlem blokları tasarım hedeflerine göre daha iyi versiyonlarla değiştirilir
    - Daha küçük Sbox, daha hızlı matris çarpımı, ...

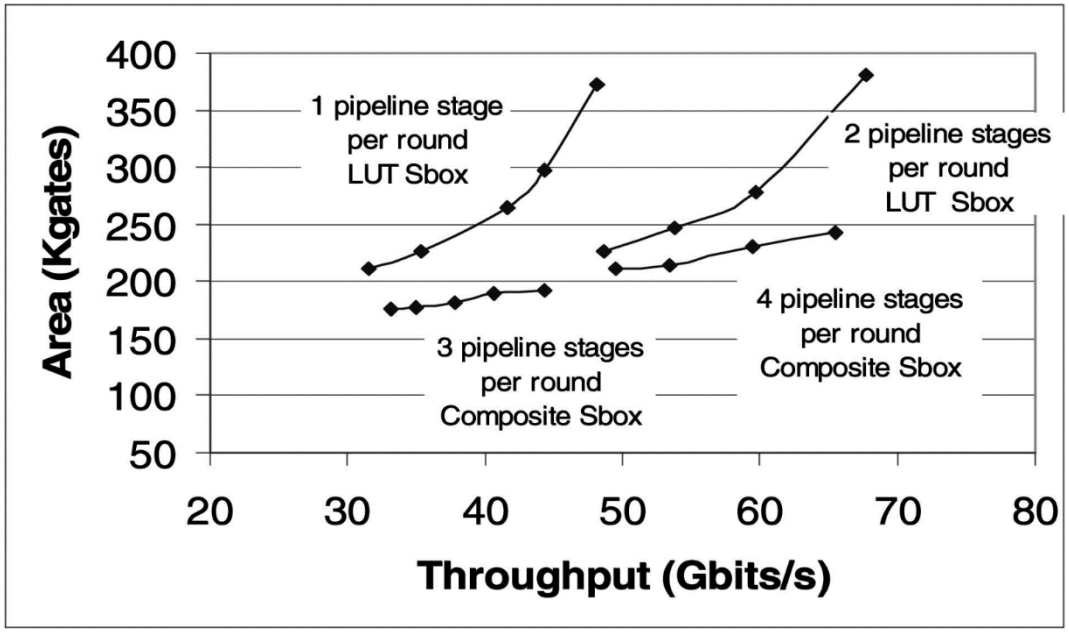
- Mimari optimizasyon
  - Paralelleştirme (2 AES devresi iki kat daha fazla veri işler)
  - Yineleme (Seri – AES state'ini bayt bazında işleme)
  - Pipelining (verimi artırma)

Donanımda Kripto Uygulamaları: AES Örneği [4]

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics



Sbox için Donanım Sentezi Sonuçları



AES Alan vs. Gecikme (Pipelining ile)

[4] Hodjat & Verbauwhede,
IEEE Trans. on Computers, 55(4), 2006

Donanımda Kripto Uygulamaları: AES Örneği [5]

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

AES-128	Throughput	Power	Gbit / s / W
Hardware (0.18 µm CMOS)	3.84 Gbit/s	350 mW	11 (1/1)
FPGA (Xilinx Virtex 2)	1.32 Gbit/s	490 mW	2.7 (1/4)
Intel AES instructions	32 Gbit/s	95 W	0.34 (1/33)
Assembler StrongARM	31 Mbit/s	240 mW	0.13 (1/85)
Assembler Pentium III	648 Mbit/s	41.4 W	0.015 (1/800)
C program on Embedded Sparc	133 Kbit/s	120 mW	0.0011 (1/10,000)
Java on Embedded Sparc	450 bit/s	120 mW	0.0000037 (1/3,000,000)

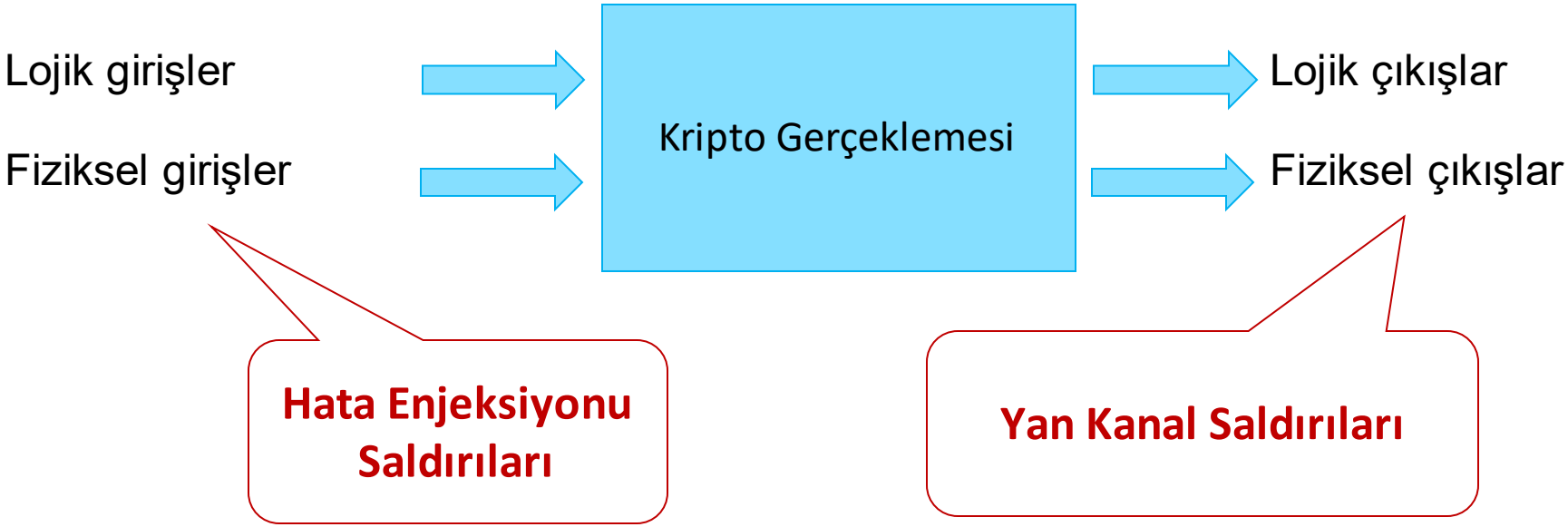
[5] Verbauwhede, 2016 TRUDEVICE Training School dersinden

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

- Donanım üzerinde kripto algoritmalarının güvenli gerçeklenmesi
  - Yan kanal analizine karşı ek güvenlik çözümleri
  - Hata enjeksiyonuna karşı ek güvenlik çözümleri

Klasik Saldırılar

Fiziksel Saldırılar



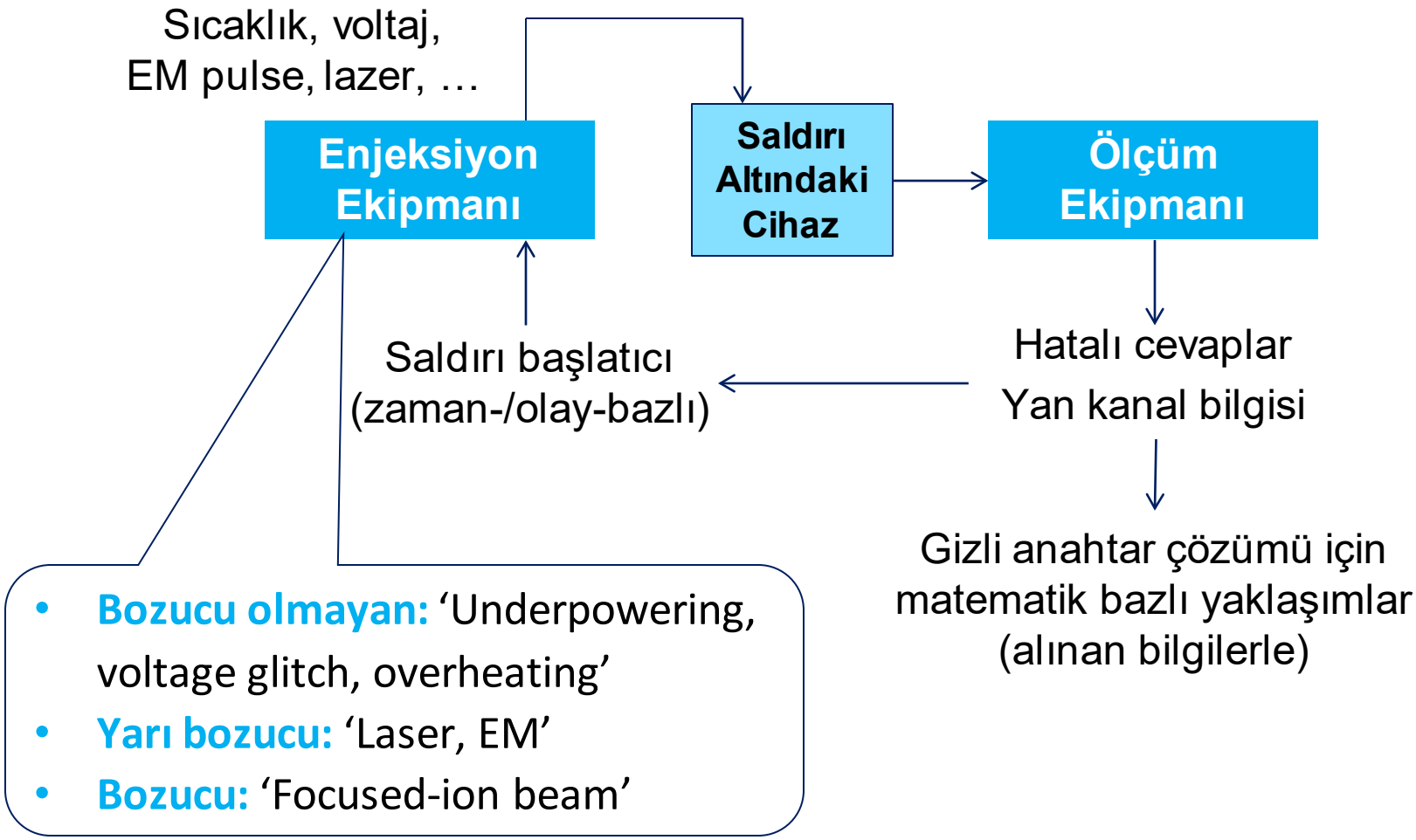
Fiziksel Saldırılar: Bozucu, Yarı bozucu, Bozucu olmayan

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

Bozucu Saldırılar	Bozucu Olmayan Saldırılar	Yarı Bozucu Saldırılar
Tersine Mühendislik (Reverse Engineering)	***Yan Kanal Saldırıları (Side Channel Attacks)***	***Optik Hata Enjekte Saldırıları***
Mikroproblama (Microprobing)	Kaba Kuvvet Saldırıları (Brute Force Attacks)	Optik Yan Kanal Saldırıları
	Hata Oluşturma Saldırıları (Fault Injection Attacks)	İleri Görüntüleme Saldırıları (Advance Imaging Attacks)
	Veri Kalıntısı Saldırıları (Data Remanence)	Ultraviyole (UV) Saldırıları

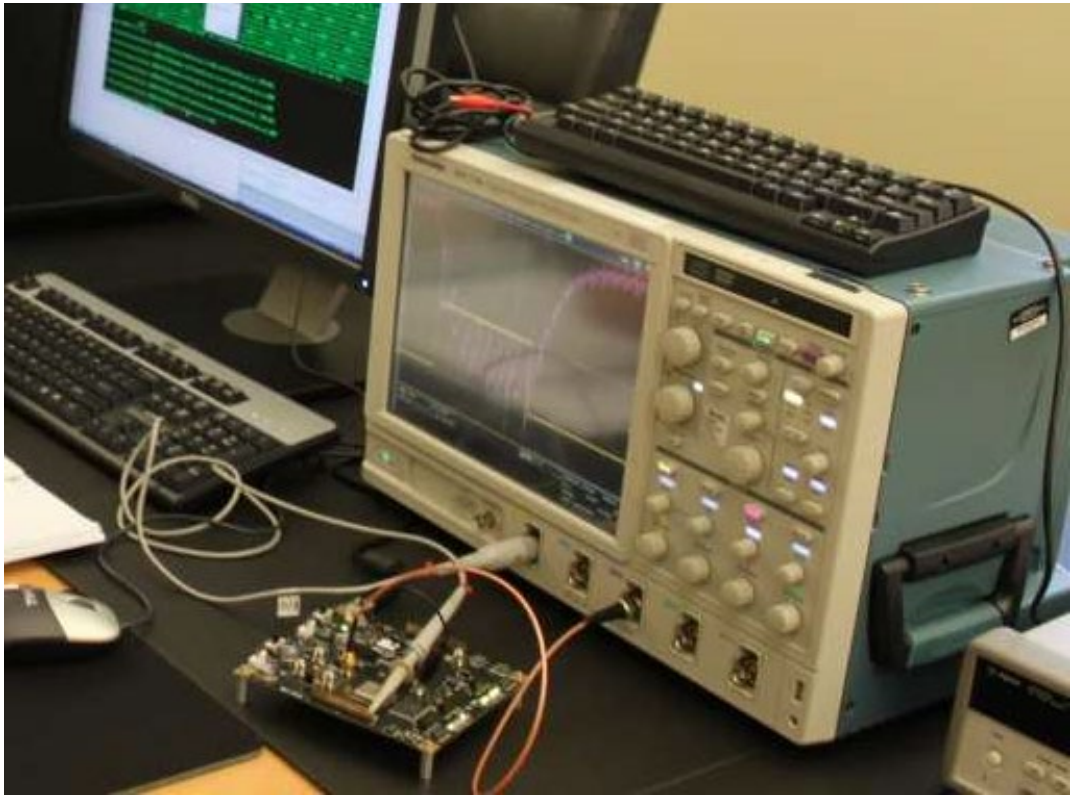
- Bir şifrenin donanım uygulamasını hedeflenir
- *Fiziksel bir bozulma* tarafından devreye enjekte edilen bir hata ile şifreleme/deşifreleme yapılır
  - Lazer, voltaj yükselmesi, clock hatası, aşırı ısınma vb.
- Toplanan/gözlemlenen sonuçlarla diferansiyel kriptanaliz yardımıyla gizli anahtar türetilir
- Bazı şifreleme dışı sistemlere de uygulanabilir
  - Sonuç bitini tersine çevirerek şifre kontrol rutinini atlama
- Son çalışmalardaki saldırılar, birkaç hata enjeksiyonu ile son teknoloji şifreleri kırabiliyor
  - Ancak uygulama çok yüksek zaman ve konum hassasiyeti gerektirir

Hata Enjeksiyonu Saldırıları - Ekipman



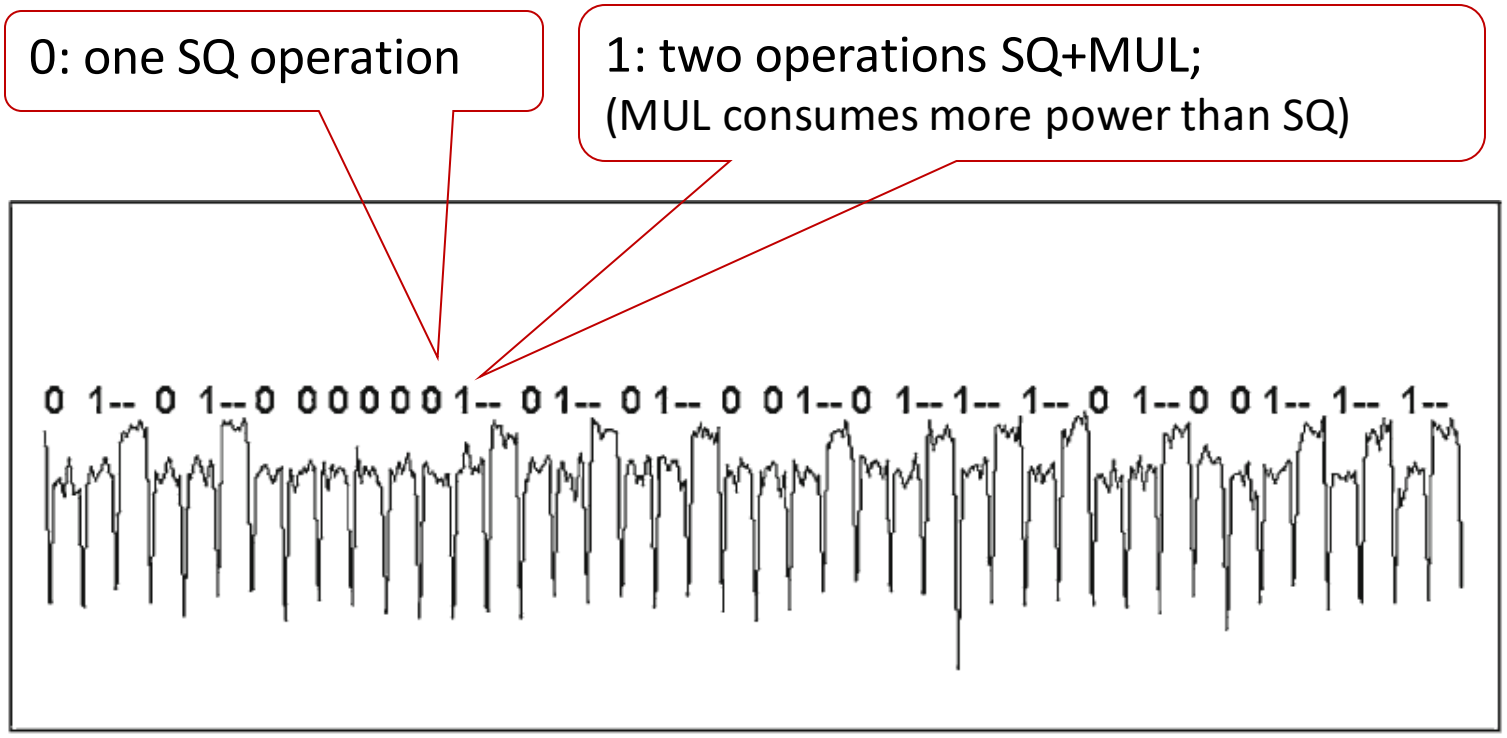
	Saldırı Önleme	Saldırı Anlama
Low-level	• On-chip clock üretimi • On-chip Vdd üretimi	• Voltaj, sıcaklık, optik, clock sensörleri
High-level	• Randomization	• Redundancy • Error-detecting codes • Infective computations

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics



- Gerçeklemeyi dinleyerek anahtarı bulmaya çalışır!

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics



- Gerçekte ise çok daha kompleks ve fazla adımlı saldırılar mümkün!

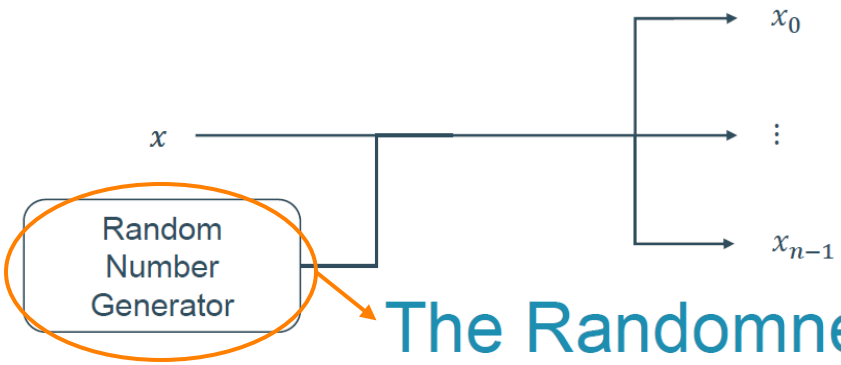
- Protokol düzeyinde karşı önlemler
  - Aynı anahtarla yapılan işlem sayısını sınırlanır
- Sızıntı azaltma
  - Dengeleme: İşlenen verilerden bağımsız güç tüketimine sahip kapılar kullanılır (örn. MDPL, WDDL)
  - Gürültü ekleme: Değişken güç tüketimine sahip devreler eklenir, zamanlamayı ve yürütme sırasını rastgele hale getirir

    - Saldırgan ise daha fazla 'iz' toplayarak veya sinyal işleme yoluyla (bir dereceye kadar) bunların üstesinden gelebilir

- Blinding (açık anahtarlı sistemler için):
  - Gizli parametrelerin matematiksel gösterimini rastgele değiştirme (nihai sonucu değiştirmeden)
  - Örn. $A \bmod P$ 'nin $A \bmod (kP) \bmod P$ ile değiştirilmesi

- Maskeleme (gizli anahtarlı sistemler için):
  - x ile hesaplama yapmak yerine, $x \oplus R$ (Boolean masking) veya $x + R \bmod 256$ (additive masking) kullanılır (R bir RNG tarafından üretilen rastgele bayt)
  - Tüm anahtar bitlerini ve round ara değerleri maskelenmiş biçimde saklanır
    - Doğrusal olmayan hesaplamalar için özel işlem gerekir
  - Saldırgan daha fazla 'iz' ile daha yüksek dereceli güç analizi yapabilir

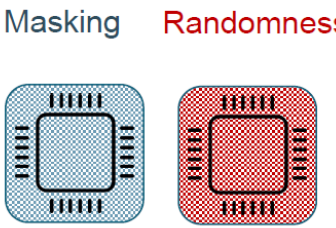
UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics



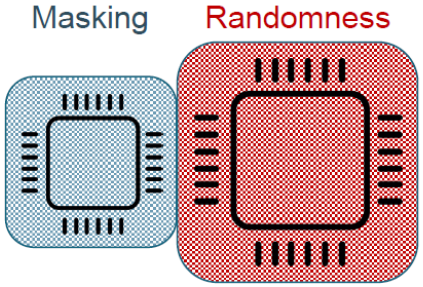
The Randomness Cost

- An example AES masking from De Cnudde et al.
  - Uses an unrolled PRINCE to generate randomness

First-Order



Second-Order



Paper cheat sheet

1. De Cnudde et al.: Masking AES with d + 1 Shares in Hardware

*** Slide Credit:** Siemen Dhooghe, COSADE'23 Keynote Talk

- Kriptografik algoritmaların sadece matematiksel tasarımı değil, sızdırma yapmayacak şekilde gerçeklenmesi de önemlidir!

- Karşı önlemler maalesef devre tasarım ölçütlerini genellikle olumsuz etkiler

- Bu tip önlemler tasarım aşamasında göz önüne alınmalıdır
  - Detaylar bir sonraki sunumda ☺

UNIVERSITY OF PASSAU

Faculty of Computer Science and Mathematics

Dinlediğiniz için teşekkürler!