Extracting Keys from Mobile Devices With Differential Power Analysis

www.cryptography.com

425 Market St., 11th Floor, San Francisco, CA 94105

CRYPTOGRAPHY RESEARCH
a division of Rambus

About Cryptography Research, Inc.

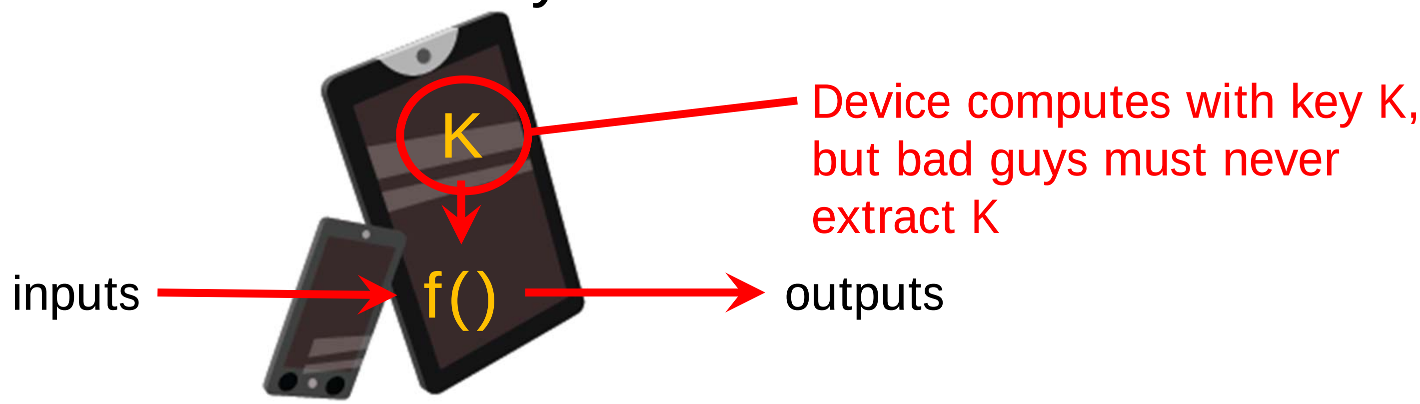
- CRI is the leading semiconductor security R&D and licensing company
  - >6 billion products are made annually with tamper resistance technologies licensed from CRI
- Defense focus: fraud, counterfeiting & digital piracy
  - Anticipate long-term trends, deploy practical and effective solutions

San Francisco HQ

Systems designed by CRI engineers secure hundreds of billions of dollars in commerce annually

Tamper-resistance

- Devices using secret or private key cryptography need to protect their secret keys



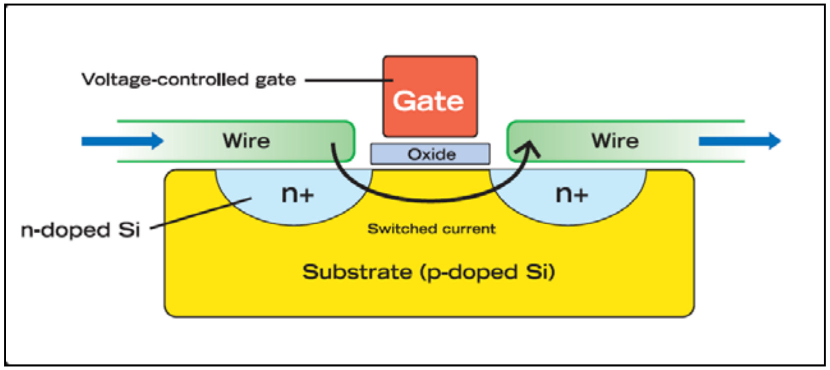
- Building block for many applications

- Payments
- Identity
- Anti-counterfeiting
- Anti-piracy
- Communications
- (and more)

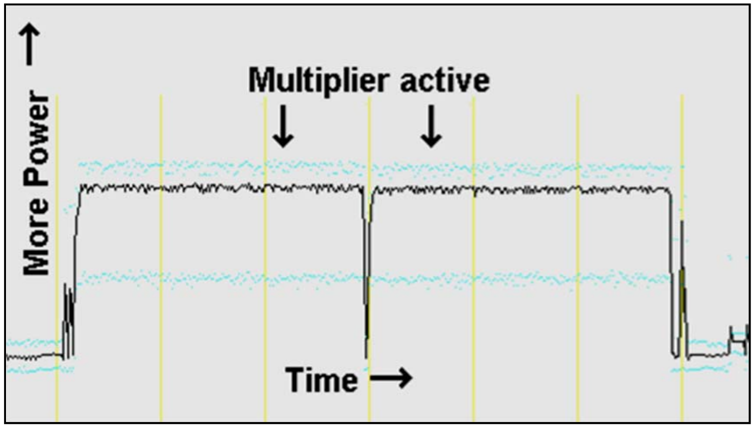
Introducing Side Channel Analysis

Crypto ops consume power

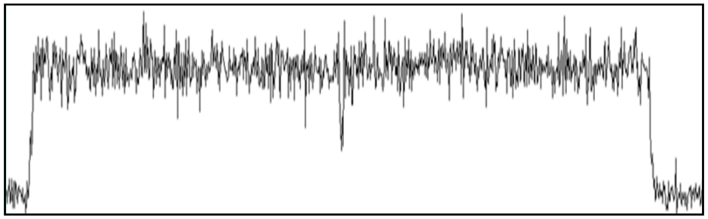
Integrated circuits contain transistors, which consume electricity as they operate.



NMOS (N-Channel) Transistor



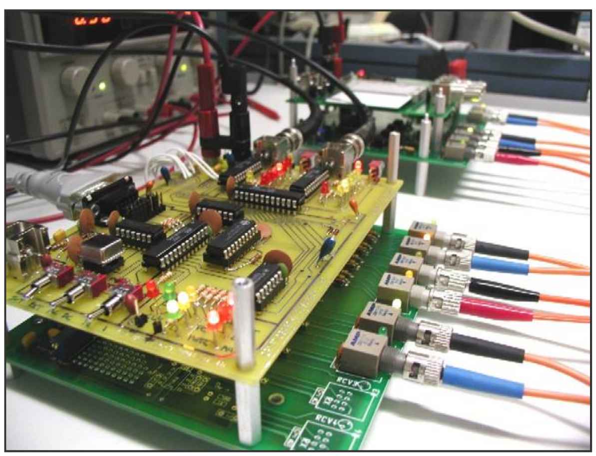
Power Consumption (RSA operation)

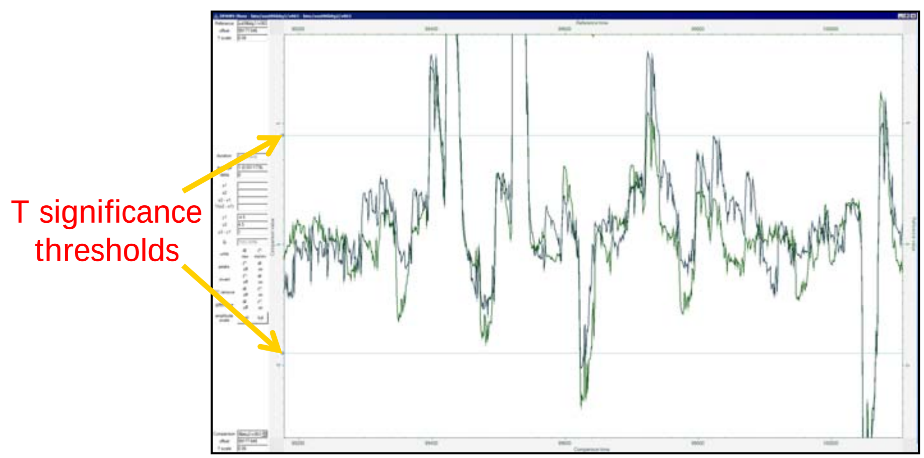


EM emission (RSA operation)

Side channel attacks

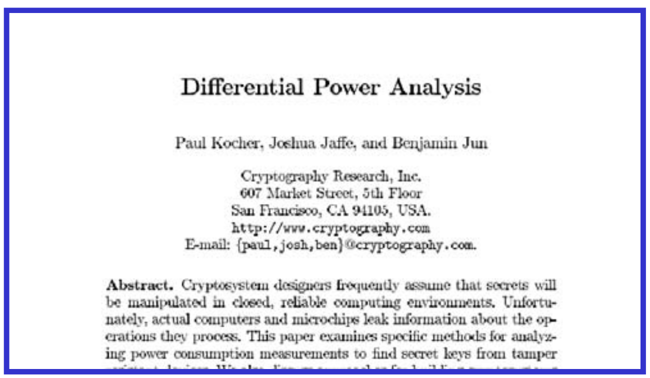
- Attacks that monitor variations in the power consumption or electromagnetic (EM) emissions of a device
- Results in full extraction of cryptographic keys from crypto HW + SW
  - Devices without countermeasures are vulnerable
- Attacks are low cost, non-invasive, passive, and leave no trace
  - Devices operate normally
  - Attack can be made at a distance with simple oscilloscope and PC (<$1,000)





Simple Power Analysis, Differential Power Analysis

- Discovered by Cryptography Research in mid-1990s (“DPA” and “SPA”)
- All cryptographic algorithms vulnerable
  - Symmetric crypto: DES, AES, HMAC,...
  - Asymmetric crypto: RSA, DH, EC variants,...
- Affects all types of hardware and software implementations, including:
  - ASICs, FPGAs, smart cards, smart phones,...
- Same techniques work for different signal sources, including timing, E&M and RF



Differential Power Analysis

Paul Kocher, Joshua Jaffe, and Benjamin Jun

Cryptography Research, Inc.
607 Market Street, 5th Floor
San Francisco, CA 94105, USA.
http://www.cryptography.com
E-mail: {paul,josh,ben}@cryptography.com.

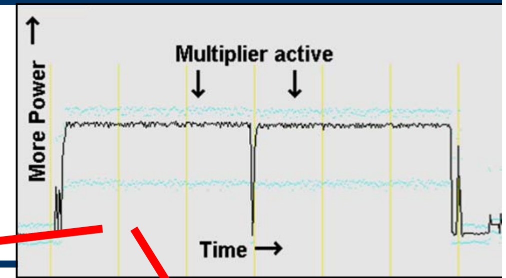
Abstract. Cryptosystem designers frequently assume that secrets will be manipulated in closed, reliable computing environments. Unfortunately, actual computers and microchips leak information about the operations they process. This paper examines specific methods for analyzing power consumption measurements to find secret keys from tamper

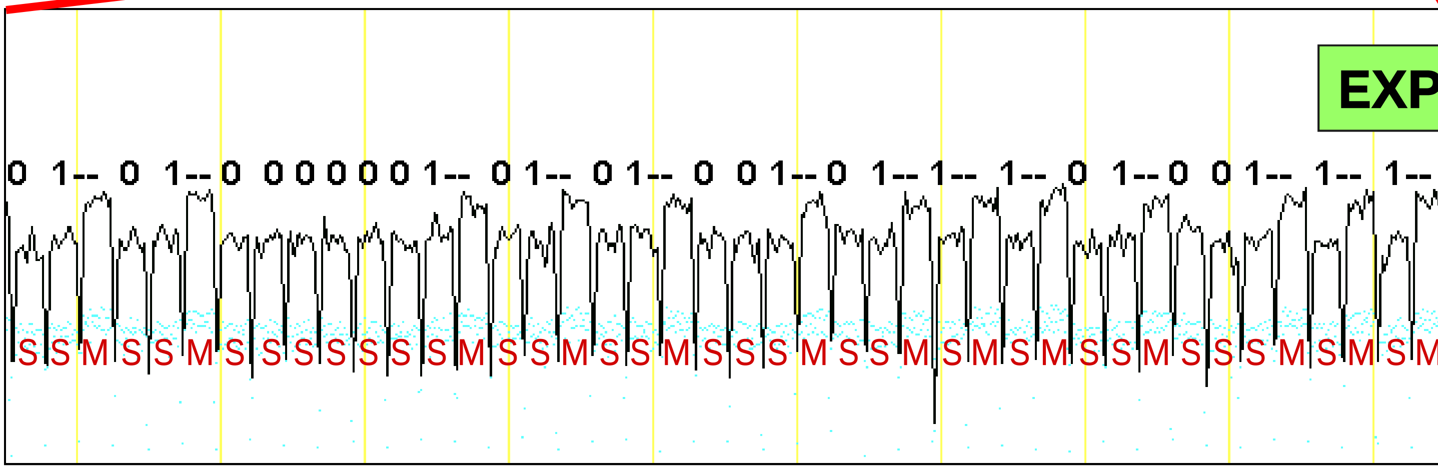
Advances in Cryptology – Crypto 99 Proceedings, LNCS 1666, Springer-Verlag, 1999

Early DPA Testing Apparatus (NYT 6/22/98)

Simple Power (EM) Analysis

Simple Power Analysis (SPA)





EXPONENT!

```
Algorithm MODULAR_EXPONENTIATION (exponent e, base b, modulus n)
      Let A = 1
      Let X = b mod n
      Let k be the number of bits in e.  Then,
      For i = k downto 0, do
            A = (A * A) mod n
            Let eᵢ be the i'th bit of exponent e        ; bit 0 is LSB
            if (eᵢ == 1), do
                  A = (A * X) mod n
            Done
      Done
      Return A
End Algorithm
```

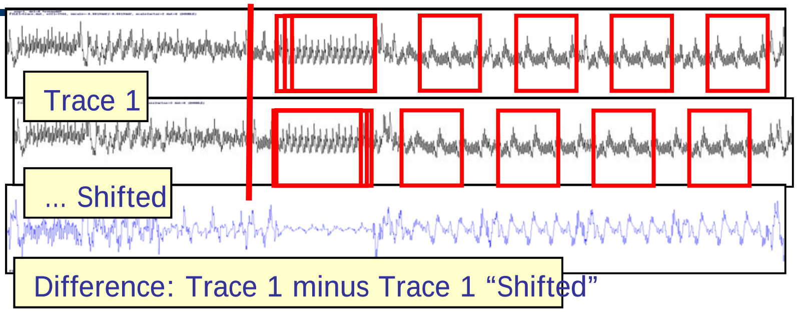
LOOP

SQUARE

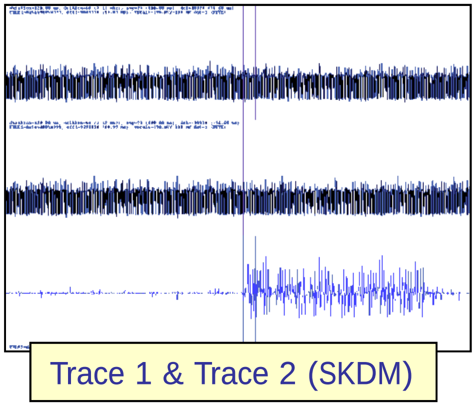
CONDITIONAL MULT

SPA as a reverse engineering tool

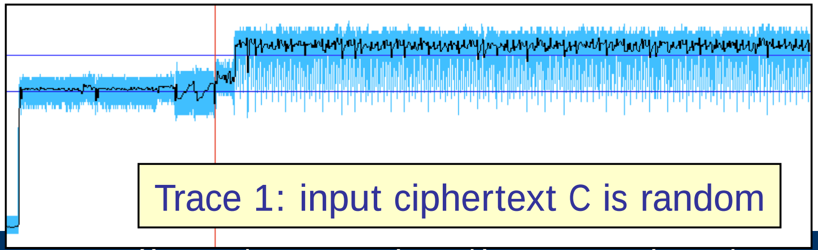
- Single-trace analysis
  - Identify loops/repeated operations
  - Shift and compare

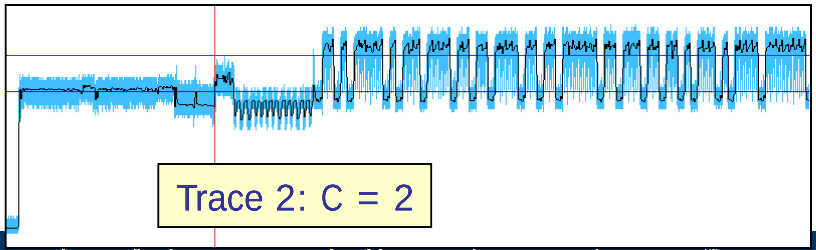


- Trace pair analysis
  - Identify differences between traces if key or message is changed

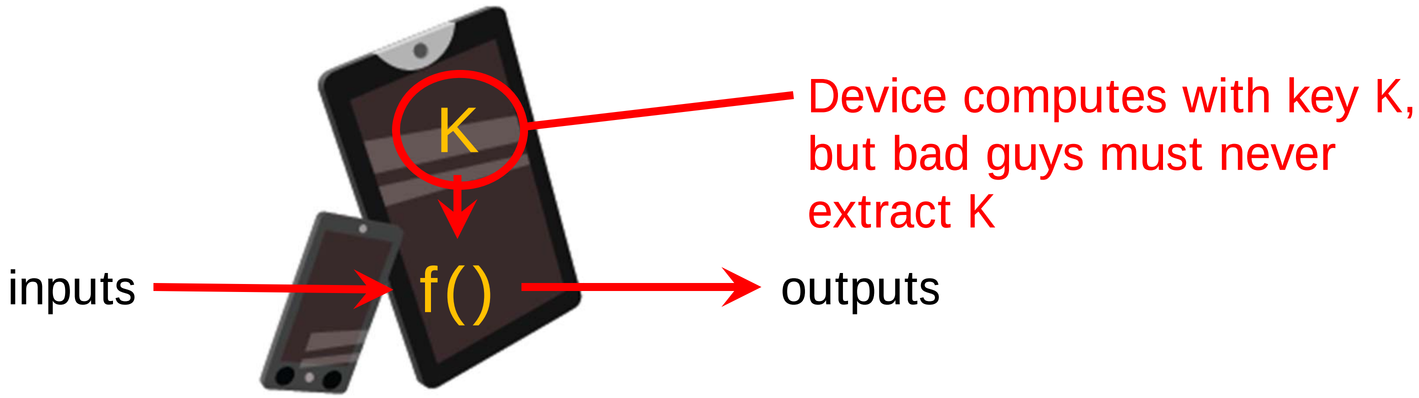


- Chosen message analysis
  - Trace pair analysis with deliberately chosen messages
  - Target: leaks for boundary conditions





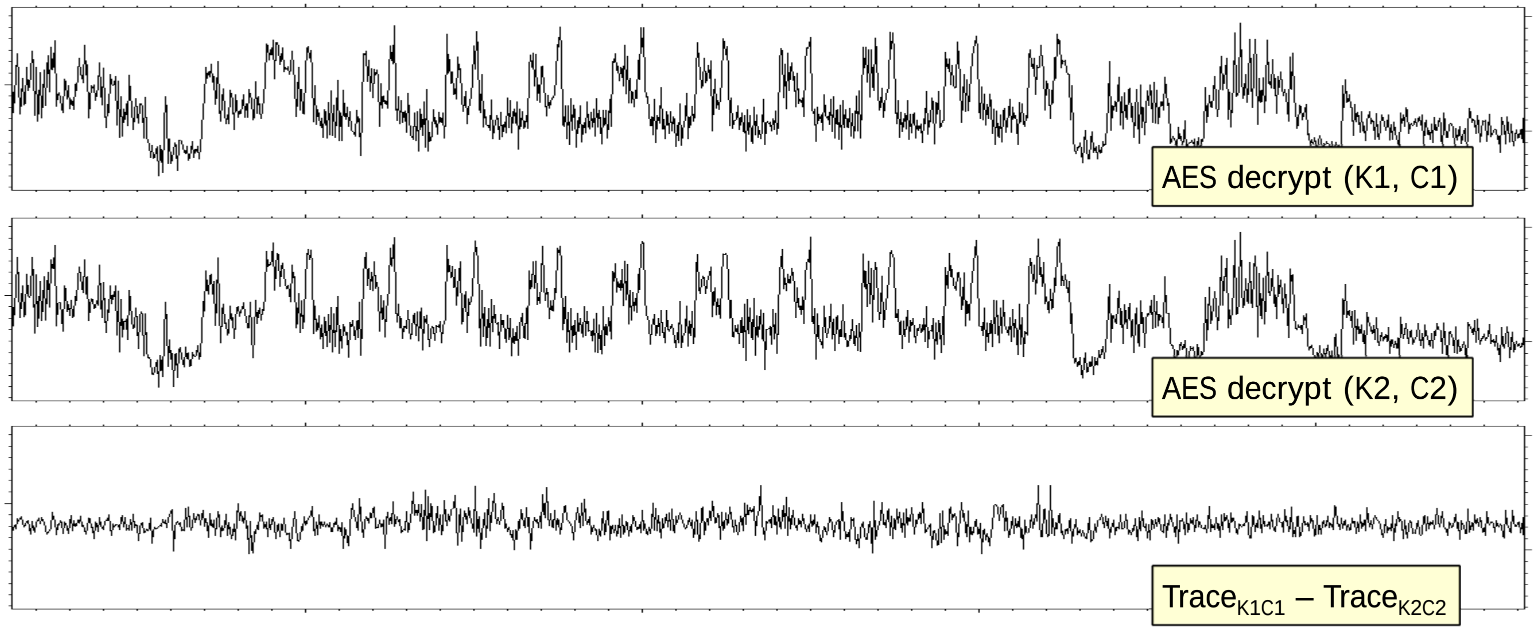
What can you do with an extracted key?



- Clone an identity device
- Forge a payment
- Pirate digital content
- Manufacture a counterfeit device
- Eavesdrop on communications
- ... and more

Differential Power (EM) Analysis

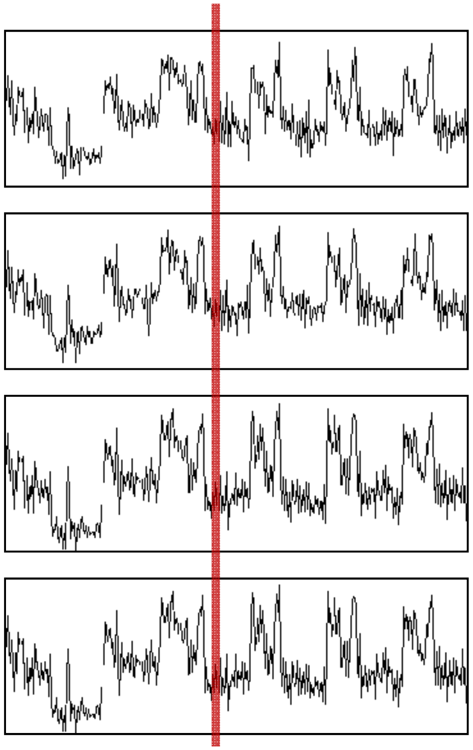
Motivation for DPA: Statistical leaks!



- With different key, different input, the general shape of AES decryption traces look similar: no obvious dependence on key or data
  - Differences outside of AES region come from noise
  - Variation within the AES operation looks a little higher, but is that significant?
- Are key and data-dependent power variations still present?

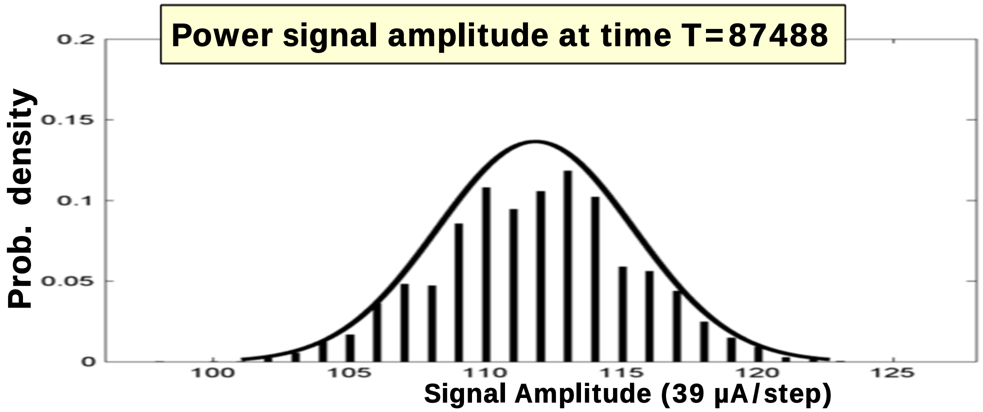
Data-dependent power consumption

- Can we isolate data dependent leakage?
- Consider a set of AES decryption traces with varying key and ciphertext



T = 87488

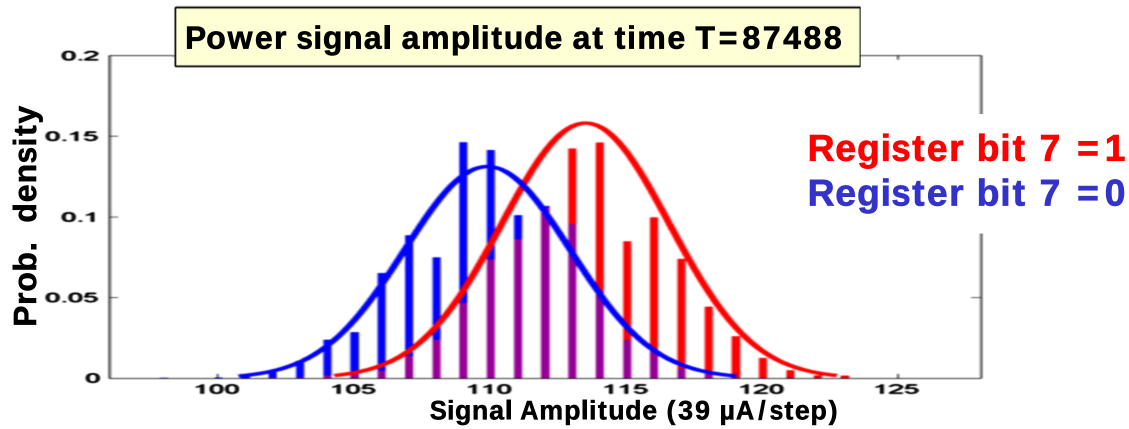
Examine distribution of power measurements at T = 87488



Does the distribution vary based on the data being processed?

Data-dependent power consumption

- What is the influence of one intermediate bit on power consumption?
- Example: Partition traces into two subsets, based on whether bit 7 in a particular register is either 0 or 1 during first round
  - Compute distribution of measurements separately for each subset

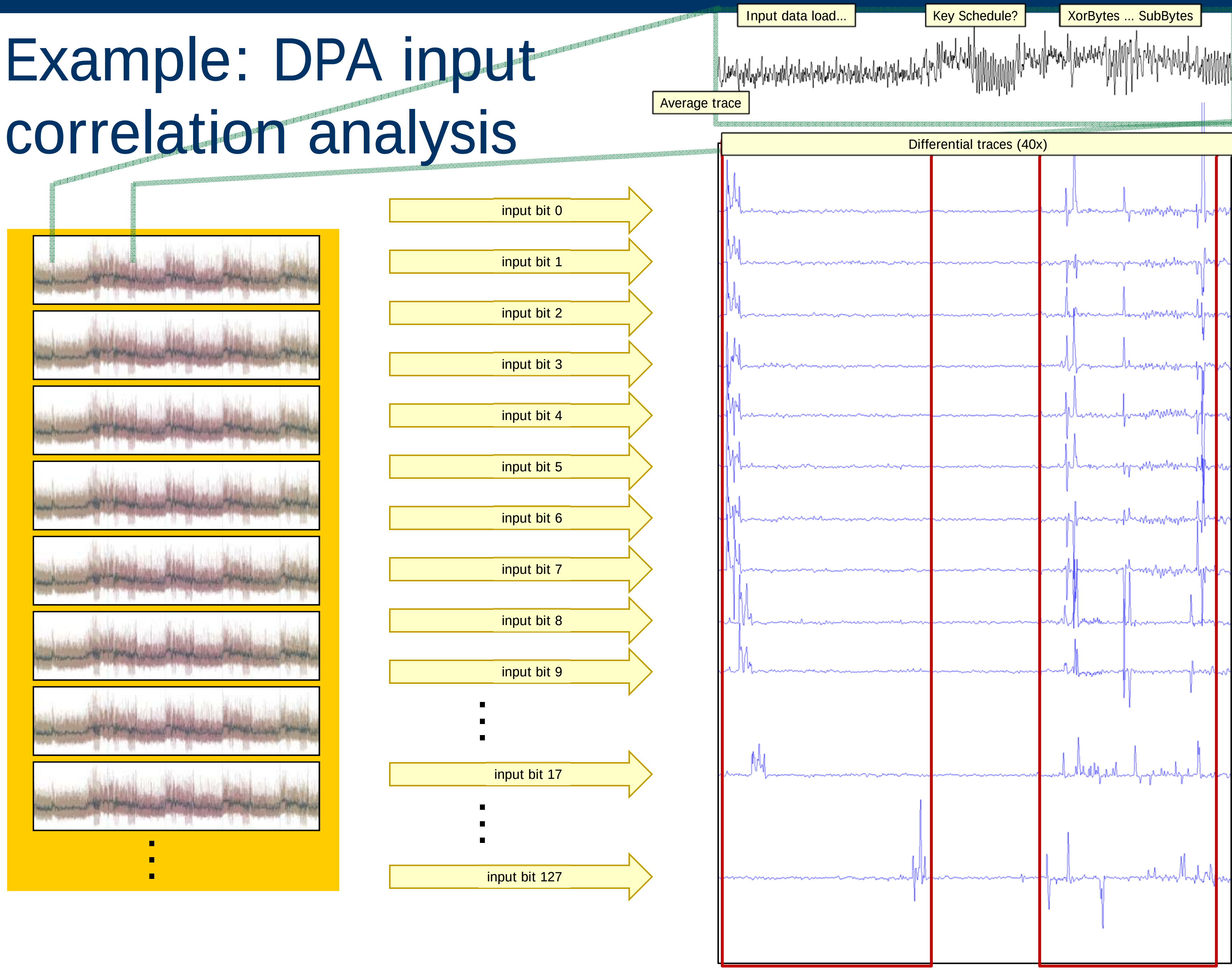


- Distribution of measurements when this bit is 0 is markedly different from distribution when bit is 1
- Probability this difference happened by chance is low: 10^{-300}

Differential Power Analysis (DPA)

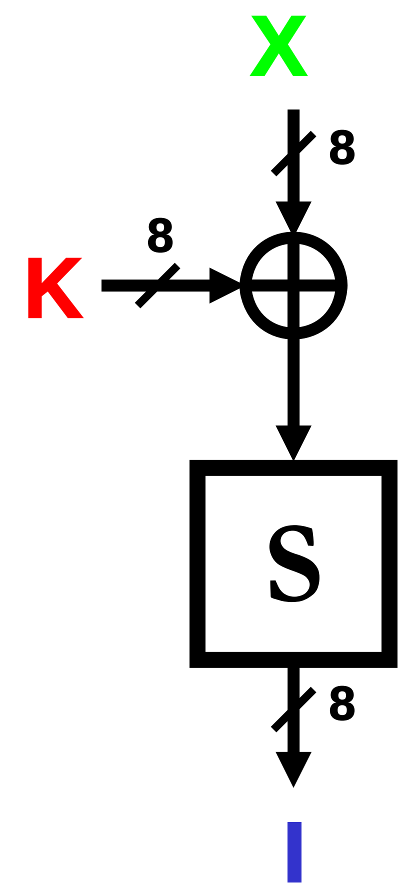
- DPA tests the question: "Do variations in processing state cause detectable variations within a set of side channel measurements?"
- DPA test process:
  - Perform multiple operations on a device with differing data
  - Measure power consumption and record (known) data processed during each operation
  - Partition set of power measurements into subsets, according to a property—such as a data bit value—of the state being processed
  - Check for statistical differences between the subsets
    - Typically difference of means
    - Vector approach: repeat the difference calculation at each offset along the traces; and view the results as a "difference trace"
- Result:
  - Differences of means shows spikes when a data leak has been isolated!
  - Spikes occur at time offsets where the device's state leaks

Example: DPA input correlation analysis

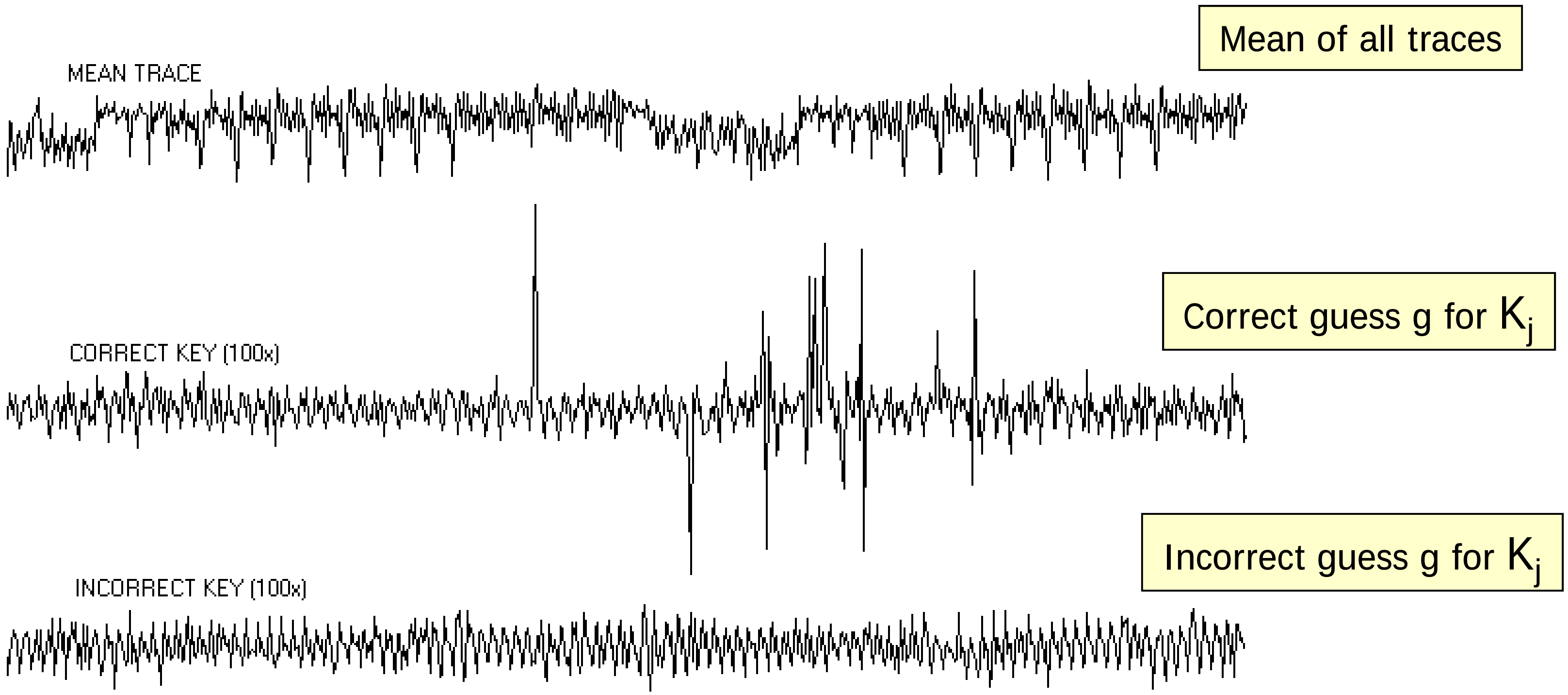


Example: DPA targeting AES Keys

- Sort and average signals based on intermediate values derived from known input and key byte
  - Guess 8-bit key K, predict bit of intermediate I for known input X
  - For each key guess (256 total), partition and average traces based on prediction of bit of I
  - Exactly 1 out of 256 key guesses will be correct
- For correct key guess, predicted I is correct and difference of averages will show peaks!



Differential Power Analysis (DPA) result



- To read more about DPA
  - www.cryptography.com/dpa
  - www.dpabook.org

Side channel vulnerabilities in mobile devices

Overview

- Increased usage of cryptography in smart-phones
  - Payments, encrypted storage, VPNs, SSL, content protection, etc
  - Security requirements in financial, enterprise, govt, content
- CPUs in smart-phones emit electromagnetic (EM) radiation during data processing
  - All tests performed with mobile device in airplane mode

CRYPTOGRAPHY RESEARCH
a division of Rambus

Capturing EM from PDA's/Smartphones

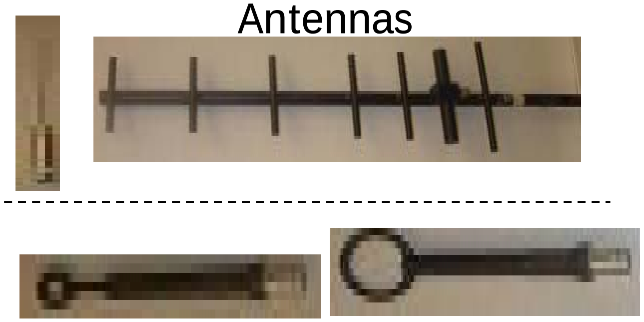
- Simple EM attack with a radio
- Usable signals even at 10 feet away

Devices

far field

near field

Antennas



Receiver ($350)

Digitizer, GNU Radio peripheral ($1000)

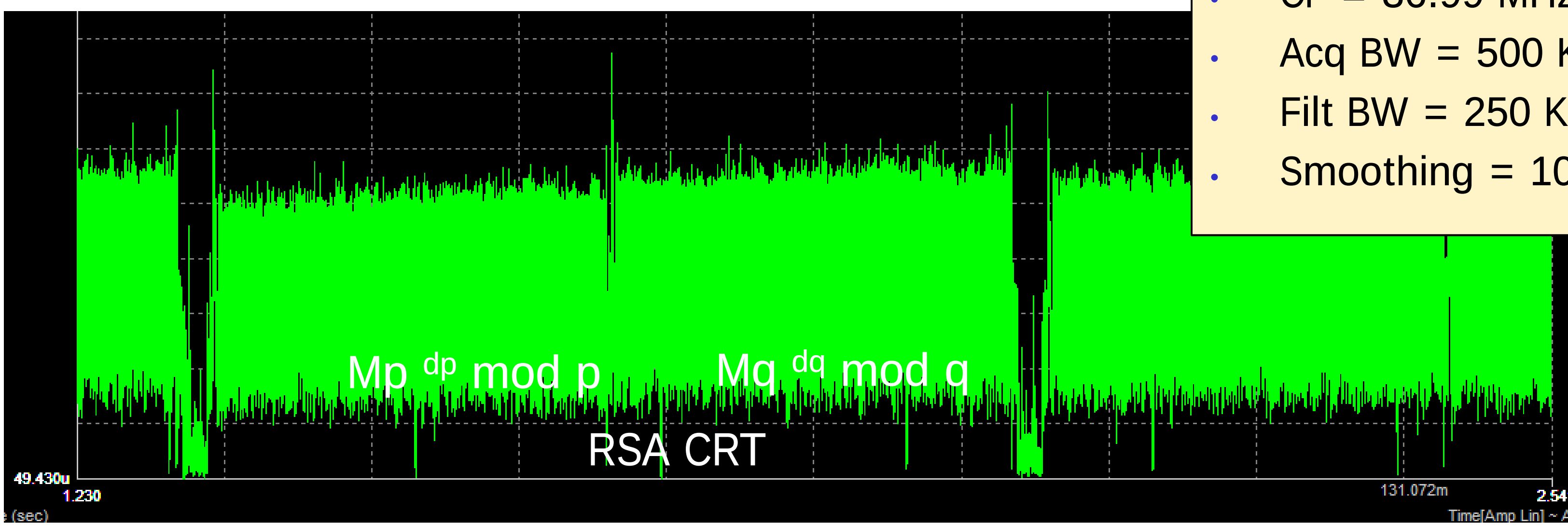
Signal Processing
(demodulation, filtering)

DPAWS™ side-channel analysis software

M-field attack on RSA

- App with simple RSA CRT implementation on mobile phone
- Magnetic field pickup coil placed behind phone
- Measurements collected during computation of

$M^d \bmod N$



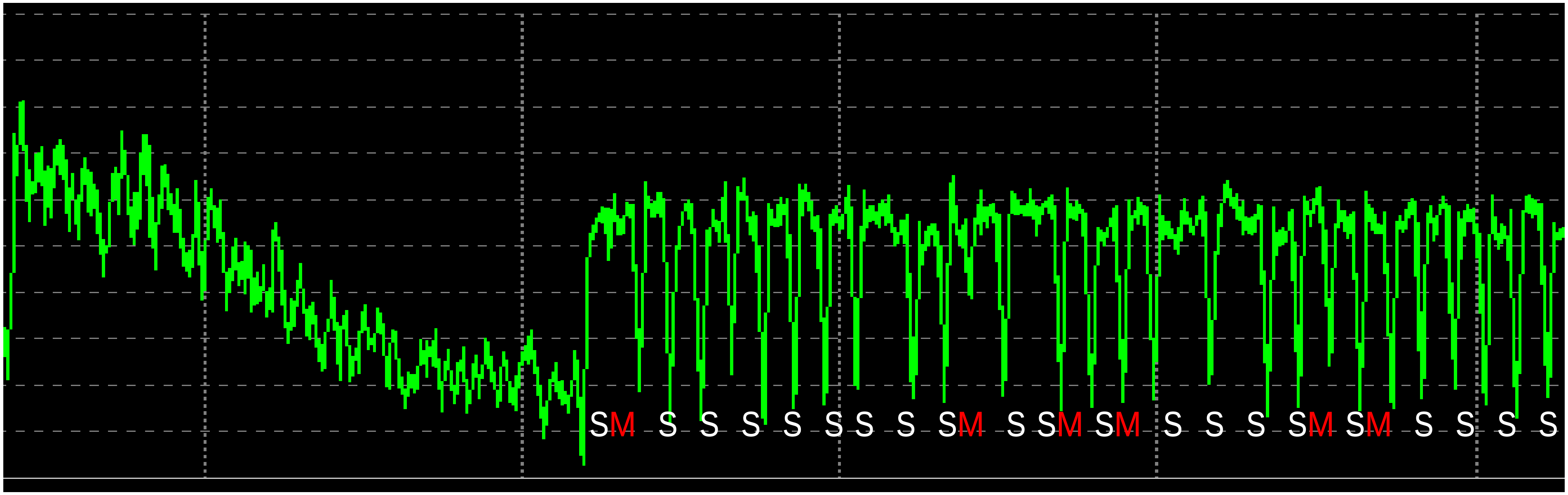
- CF = 36.99 MHz
- Acq BW = 500 KHz
- Filt BW = 250 KHz
- Smoothing = 10

CRYPTOGRAPHY RESEARCH
a division of Rambus

RSA: Key extraction

- Focus on Mp^{dp} mod p calculation (Mq^{dq} mod q similar)

```
For each bit i of secret dp
   perform "Square"
   if (bit i == 1)
     perform "Multiply"
   endif
endfor
```



CRYPTOGRAPHY™ RESEARCH
a division of Rambus

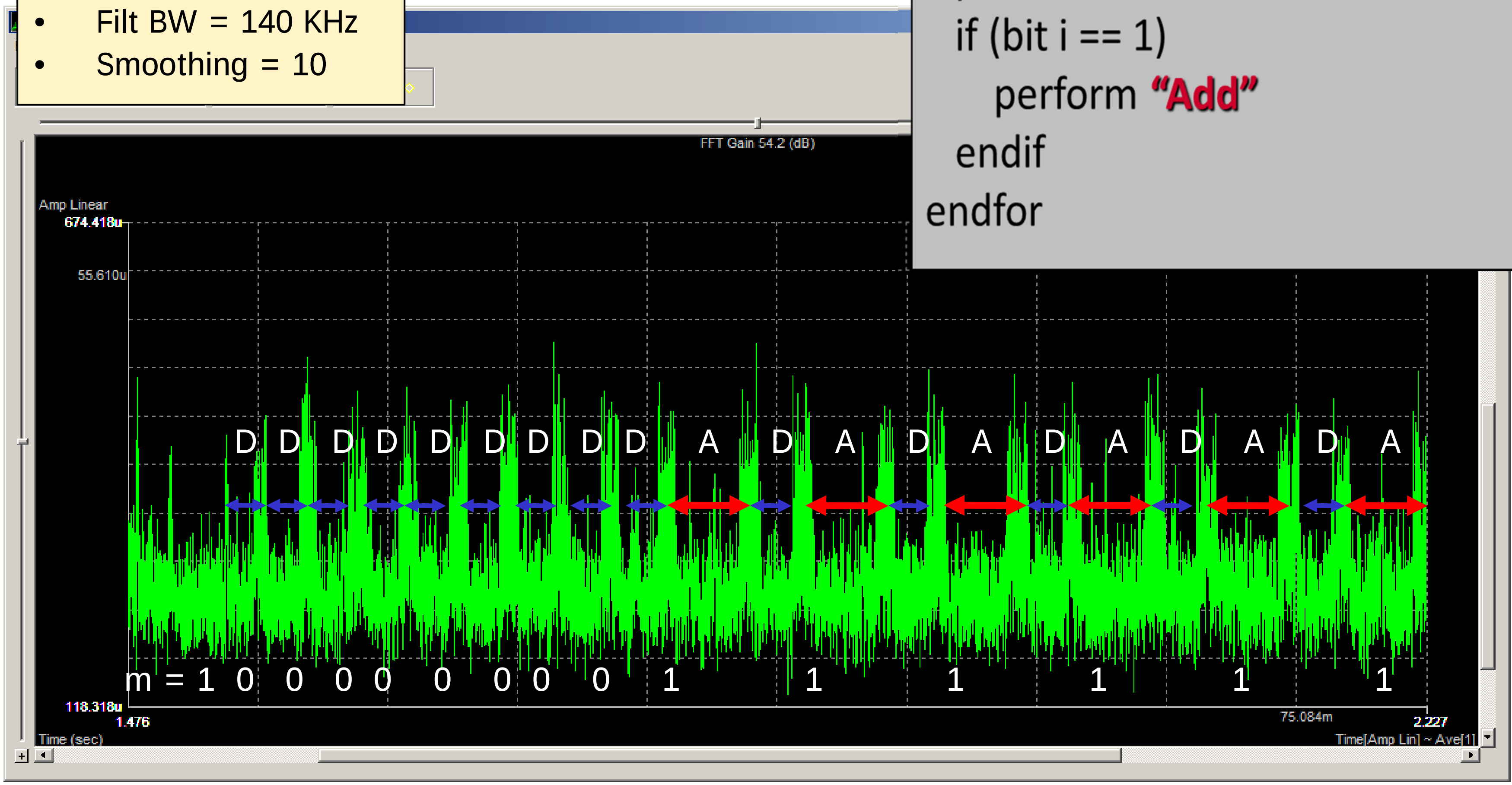
Simple EM attack on ECC from 10 feet away

- Elliptic Curve crypto app
  - Point multiplication (m * Q) over P-571 using open source crypto library
- Double-and-add algorithm to compute m*Q
  - In ECC, double and add are very different operations
  - The double/add execution sequence yields m (!)

ECC Signal: Extracting Secret M

- CF = 972.177 MHz
- Acq BW = 200 KHz
- Filt BW = 140 KHz
- Smoothing = 10

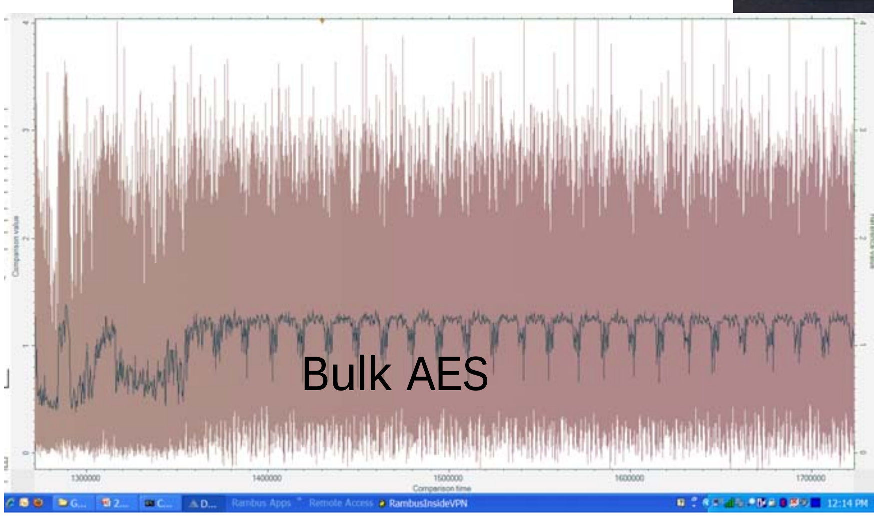
For each bit i of secret m
  perform "Double"
  if (bit i == 1)
    perform "Add"
  endif
endfor

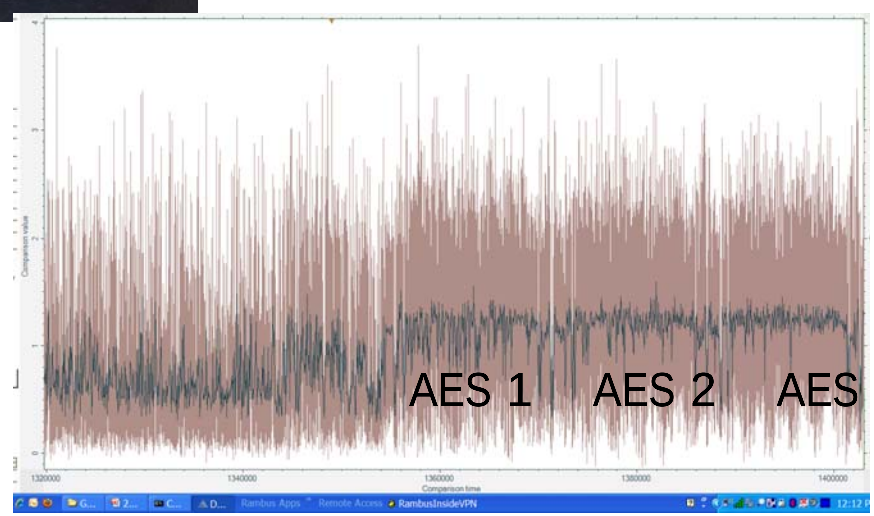


DPA attack on AES

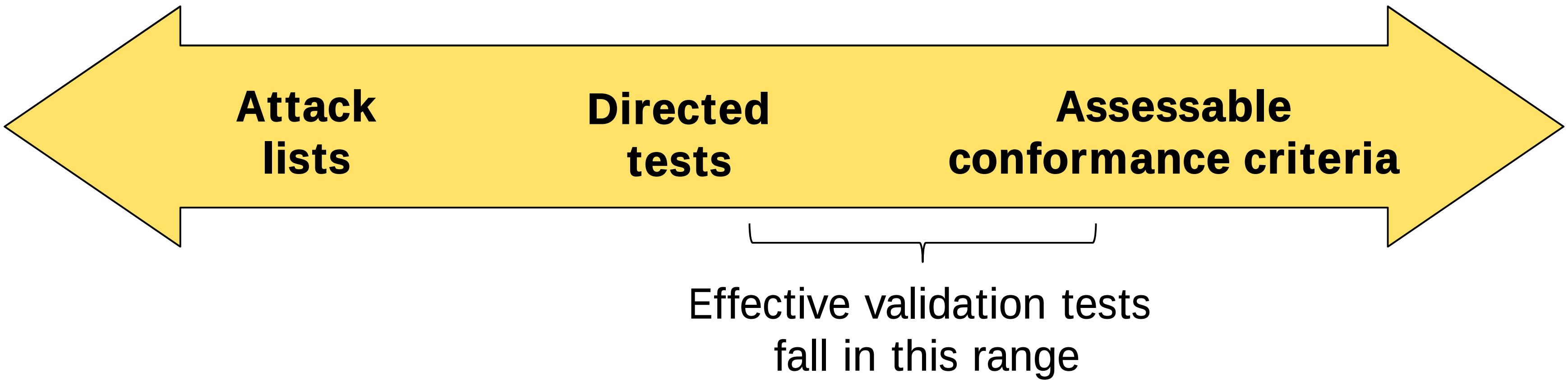
- Bulk AES encryption on another phone
  - App invokes the Bouncy Castle AES provider
  - Baseband m-field trace capture on a sampling scope

- Baseband
- Acq LPF = 100 MHz
- Filt BW = 60 MHz





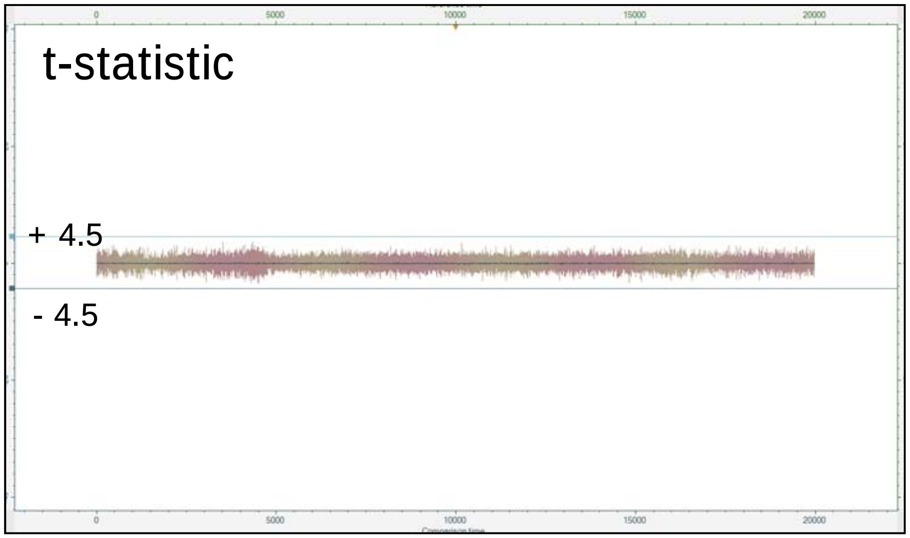
Efficient leakage testing



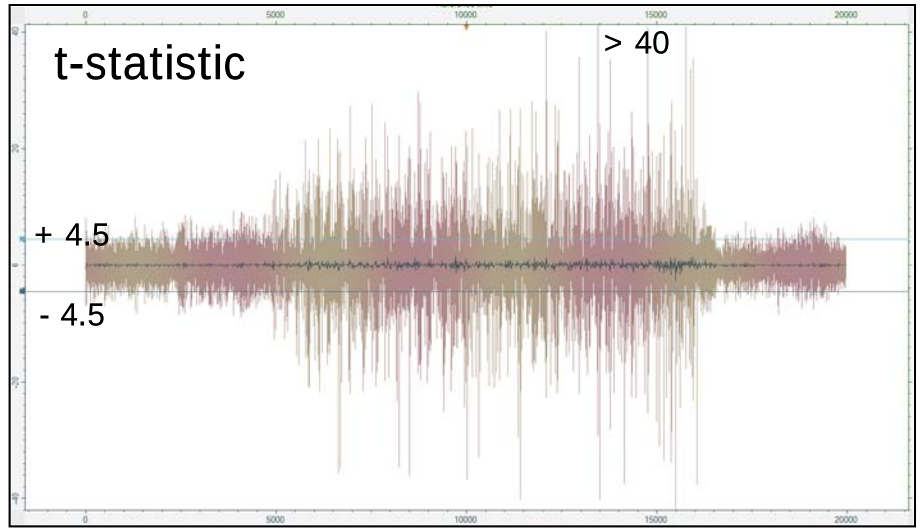
- We can test for leakage without actually doing full DPA key recovery
- Standardized tests perform statistical analysis to identify presence of leakage

Information leakage assessment on AES

- Results of standardized leakage test on leaky device



Control Group: t-test comparing
average signal from Set 1 (random AES)
with average signal from Set 2 (random AES)



Test Group: t-test comparing
average signal from Set 1 (random AES)
with average signal from Set 3 (fixed AES)

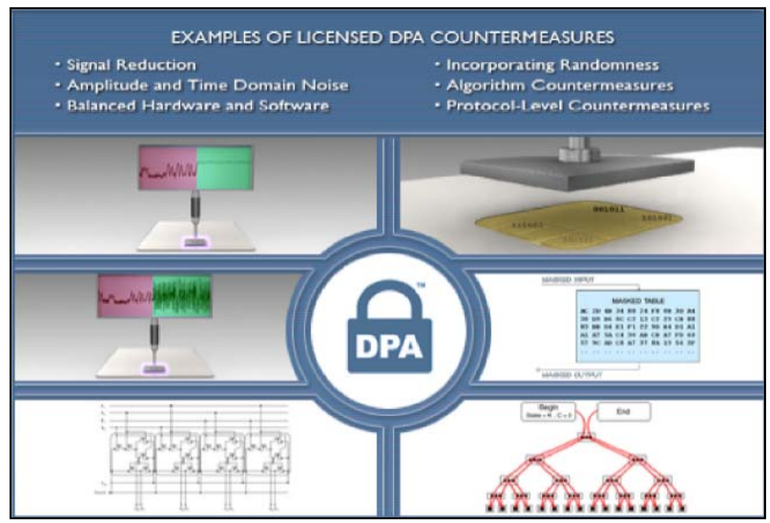
Defenses

Defenses against power analysis

- Categories
  - Obfuscation
  - Leak Reduction
  - Balanced HW / SW
  - Amplitude & Temporal Noise
  - Incorporating Randomness
  - Protocol Level CM

- Certifications / Requirements
  - FIPS 140-3 draft
  - Common Criteria
  - CAC, E-Passport, HSPD-12

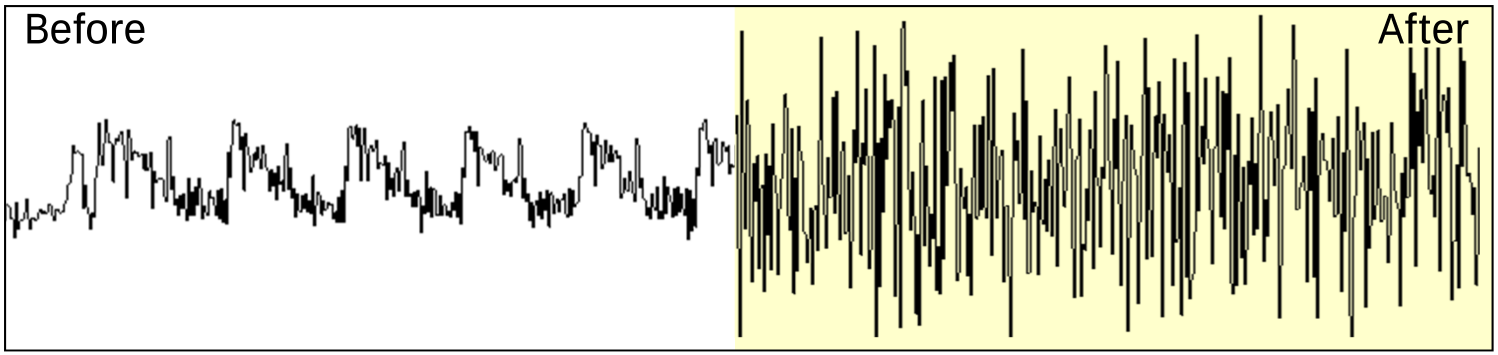
A license is required to make, use, or sell DPA-resistant devices



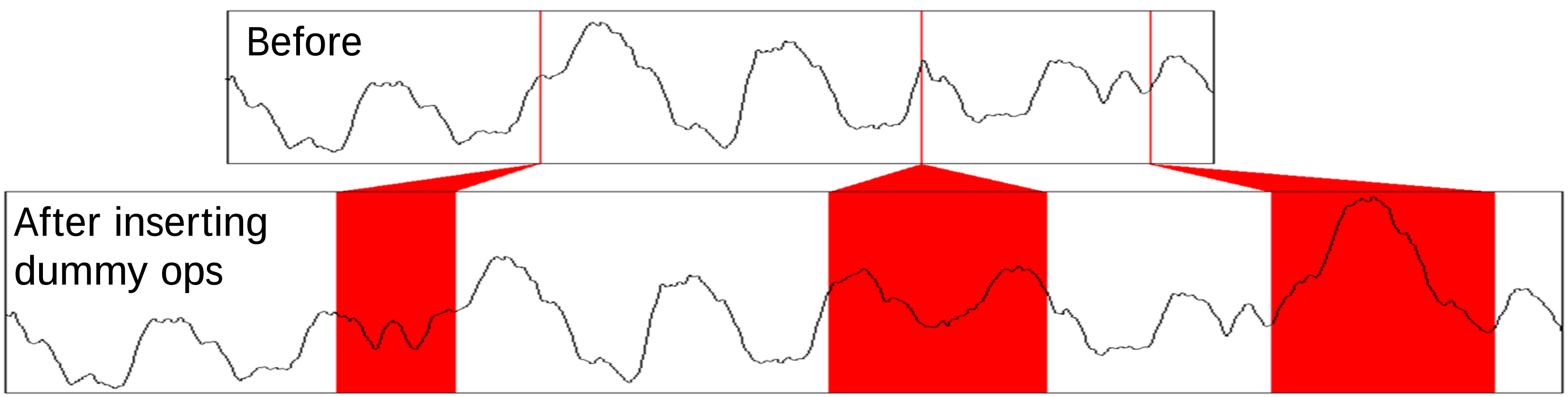
Cryptography Research

Example HW countermeasure: Noise

- Amplitude noise: Voltage spikes, fluctuations due to random data

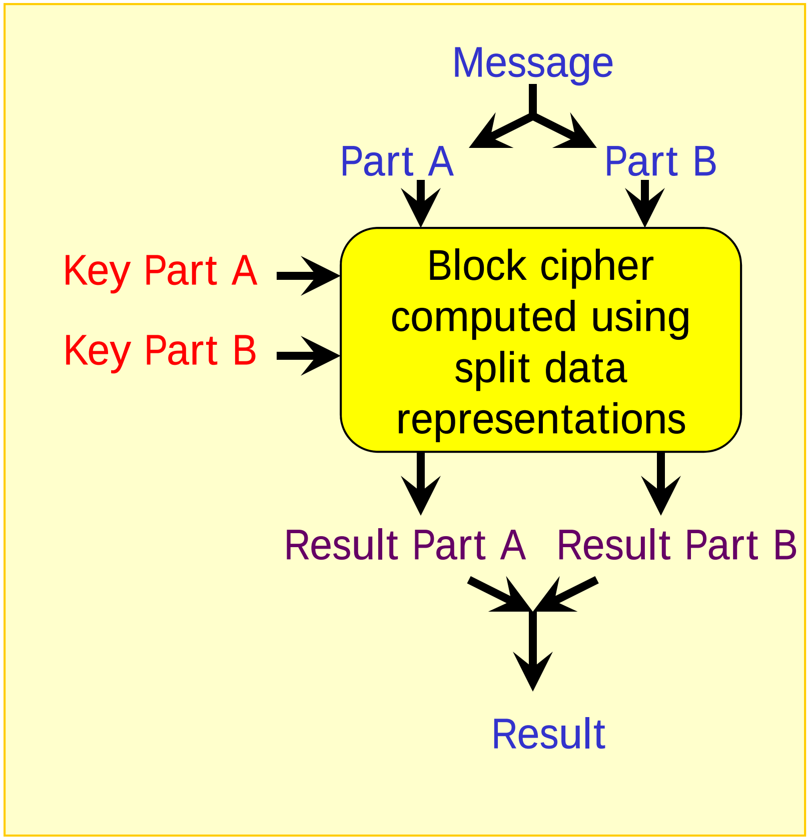


- Temporal noise: Random delays, dummy operations, randomized clock



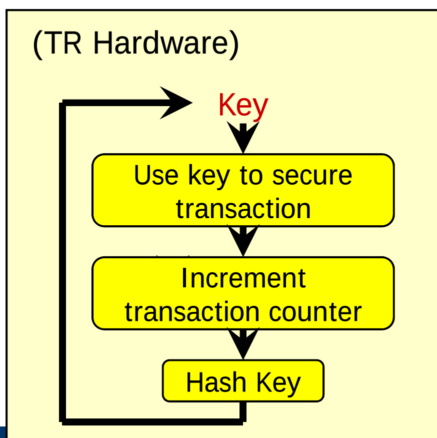
Example of a SW-friendly countermeasure: Masking

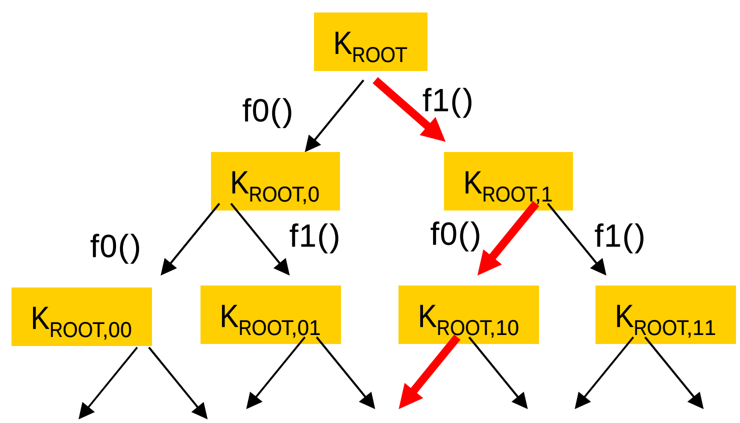
- Implement block cipher with random information to
  - Split key into two (or more) randomized parts
  - Split message into two (or more) randomized parts
  - E.g., Key = Key Part A $\oplus$ Key Part B
- Compute block cipher using the unpredictable parts
  - Correct answer is obtained, but no internal variable is correlated to the input and key



Example: Protocol level countermeasures

- Build protocols that survive information leakage
  - Design crypto with realistic assumptions about the hardware
  - Hardware has to be fairly good, but assumed to leak
  - Can obtain provable security against DPA with reasonable assumptions and significant safety margin
- Can perform symmetric key transactions, challenge response, authenticated encryption/decryption





Conclusions

- Without countermeasures, all mobile device CPUs leak information about cryptographic keys
  - Key extraction at 10 feet with $1000 of equipment

- This is a solvable problem in today's constrained devices
  - Defenses can be implemented in hardware, software, and protocol layers

- New metrics in conformance-style tests allow consistent security assessment
  - Provide direct leakage feedback to developers
  - "Red team" techniques may not be required for product assessment

Questions?

Benjamin Jun
VP and CTO
Cryptography Research Inc.

ben@cryptography.com
+1 415-390-4323

(Email me for a copy of the slides)