Differential Power Analysis

Copy Protection Technical Working Group
October 16, 2013 - Los Angeles

www.cryptography.com

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

© 2013 Cryptography Research, Inc. Protected under issued and/or pending US and/or international patents. All trademarks are the property of their respective owners. The information contained in this presentation is provided for illustrative purposes only, and is provided without any guarantee or warranty whatsoever, and does not necessarily represent official opinions of CRI or its partners. Confidential - unauthorized copying, use or redistribution is prohibited.
Meeting Agenda

• About Cryptography Research

• Simple and Differential Power Analysis

• Countermeasures
About Cryptography Research, Inc.

- CRI is a leading semiconductor security R&D and licensing company
  - Founded 1995
  - Acquired in 2011 by Rambus for $342.5 million
  - Today, over 7 billion products are made annually with tamper resistance technologies licensed from CRI
- Provider of security technologies & solutions to multiple industries
  - Including Pay TV, semiconductor, printing, government, payments
  - Designed BD+ security for Blu-ray disc format
  - Secure Content Storage Association

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

R&D and innovation for securing semiconductors and electronic systems

Expert security technology development and consulting

Differential Power Analysis (DPA) countermeasures

CryptoFirewall™ SoC IP solutions for content security & anti-counterfeiting
CRI business overview

R&D and innovation for securing semiconductors and electronic systems

Expert security technology development and consulting

Differential Power Analysis (DPA) countermeasures

CryptoFirewall™ SoC IP solutions for content security & anti-counterfeiting

Focus of the slides today
Simple Power Analysis and Differential Power Analysis
What is Simple Power Analysis and Differential Power Analysis?

• Power analysis attacks find secret keys from semiconductor devices by analyzing power consumption
  ◦ SPA attacks use direct observation of power consumption measurements.
  ◦ DPA attacks add statistical techniques that can infer keys from minute correlations within measurements across many operations.
Differential Power Analysis

- Discovered by Cryptography Research in mid-1990s ("DPA" and "SPA")
  - Thousands of research papers site CRI’s ground-breaking discovery, whitepapers, and fundamental patents

- Low cost, non-invasive attacks on crypto HW
  - Key extraction
  - Reverse engineering

- 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, EM and RF

---

Differential Power Analysis

Paul Kocher, Joshua Jaffe, and Benjamin Jun

Cryptography Research, Inc.
607 Market Street, 5th Floor
San Francisco, CA 94103, 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-resistant devices. We also discuss approaches for building cryptosystems that can operate securely in existing hardware that leaks information.

Keywords: differential power analysis, DPA, SPA, cryptanalysis, DES

---

Advances in Cryptology – Crypto 99 Proceedings, LNCS 1666, Springer-Verlag, 1999
How simple power analysis works

Integrated circuits contain transistors, which consume electricity as they operate. The total power consumption of an integrated circuit and its EM emissions depend on the activity of its individual transistors.

NMOS (N-Channel) Transistor

Power Consumption (RSA operation)

EM emission (RSA operation)
Simple Power Analysis

- Keys can be extracted from a single trace

Straightforward RSA Implementation

i.e. \( M^d \mod N \), with secret key \( d \)

For each bit of secret exponent \( d \)

- if bit == 0, perform "Square" only
- if bit == 1, perform "Square" followed by "Multiply"

endif
endfor
Demo: Simple EM analysis of RSA

- Straightforward RSA implementation on modern 4G smartphone
- Pickup coil placed behind phone collects measurements during computation of
  \[ M^d \mod N \] [d is the RSA secret key]

Iterations of the exponentiation ‘For’ loop

Trace from a phone

- CF = 108 MHz
- Acq BW = 6.25 MHz
- Filt BW = 1.25 MHz
- Smoothing = 100

bits of d: 0 1 1 0 1 1 0 0
Differential Power Analysis
DPA: Statistical techniques for extracting keys using data with low signal/noise ratio

- Signal / noise ratio may be very small
  - However, tiny statistical influence of intermediates on power consumption remains...

- Eg. Mean of signals where Register 7 bit 1 = 0 is different from mean of signals where Register 7 bit 0 = 0

- DPA: Uses statistical methods to analyze minute data dependent differences in power measurements to recover the key.
Differential Power Analysis (DPA) test

Process for testing data dependent power consumption:

- Perform multiple device operations with differing data
- Record power measurement samples/trace and known data for each operation
- Partition set of power traces into subsets, according to a data dependent property
  - E.g., data bit of an intermediate state during processing
- Calculate difference of subsets' means

Results:

- Difference trace shows spikes at time offsets wherever data dependent property affects power consumption
DPA Attack

• Perform multiple device operations with same key and differing data
• Record power measurement samples/trace and known data for each operation.
• Guess a portion of the key (Eg. $K_3$) and predict intermediates dependent on guess (Eg. $I_3$).
• Perform a statistical test to check if power measurements are influenced by predicted intermediates $I_3$.
• Just repeat for remaining key portions.
DPA Tests are extremely powerful

• With sufficiently many traces, the DPA test can isolate even the tiniest data dependent leakage
  ◦ Data bits moving on buses, wires, switches
  ◦ Data bits written to registers
  ◦ Data bits that change when a register overwritten
  ◦ Switching activity within combinatorial circuits
  ◦ A single transistor switching
  ◦ ……..
DPA Demo: AES-CBC on FPGA Fabric

- Typically AES is implemented in hardware to perform bulk encryption
  - CBC-mode or counter-mode
  - 20k block cipher operations for a 320KB buffer

- Power trace from single bulk encryption contains multiple independent AES operations with same 128-bit key

- Can use multiple AES ops from a single trace to perform DPA
Demo: Content Decryption
General principles for countermeasures

- SPA/DPA immunity is possible and practical
  - But very different from a “bug fix”
- Security can involve a mix of countermeasures
  - Hardware
  - Software & algorithms
  - Key management & protocol layer
- Overheads (performance, size, area, power) depend on
  - Algorithms being protected
  - Leakage characteristics of device
  - Desired level of immunity
  - Engineering constraints and design flexibility
SPA/DPA Countermeasures

Categories:

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

Cryptography Research has patented the fundamental DPA countermeasures
Countermeasures

• CRI licenses patents and technology for mitigating DPA and other side channel attacks
  ◦ Countermeasures can be deployed in any combination of hardware, software and protocols
  ◦ Portfolio of U.S. and foreign patents on countermeasures
  ◦ Training and evaluation services + analysis equipment
• Primary licensees: Companies that make secure products and semiconductors

Applications requiring DPA protection

- Smart cards
- Communications systems
- PDA/Cell phone DRM
- Defense
- Postage meters
- FPGAs
- POS terminals
- Video decoding chips
- Game consoles
- (and more)
Licensees, partners and standards

**LICENSEE**
- ALi
- BROADCOM
- CPU TECH
- EM MICROELECTRONIC
- infineon
- insideSECURE
- Microsemi
- Microsoft
- mkron
- NXP
- RENESAS
- Raytheon
- SAMSUNG
- VISA
- TOSHIBA
(And Others)

**PARTNER**
- AIST
- brightsight
- Applus
- ETRI
- KISA
- INFOGARD
- Keirex
- LOCKHEED MARTIN
- MITRE
- Raytheon
- riscure
- Sandia National Laboratories
- Rockwell Collins
- T Systems
- UNISYS
- THALES
(And Others)

**STANDARDS**
- Common Criteria
- EMVCo
- FIPS
- PCI Security Standards Council
- SCSA
- MasterCard
Thank You

Tom Carroux  
(650) 862-8855  
Tom.Carroux@cryptography.com

Robert Ranucci  
(951) 288-9888  
Robert.Ranucci@cryptography.com

Sami Saab  
(415) 390-4378  
Sami.Saab@cryptography.com