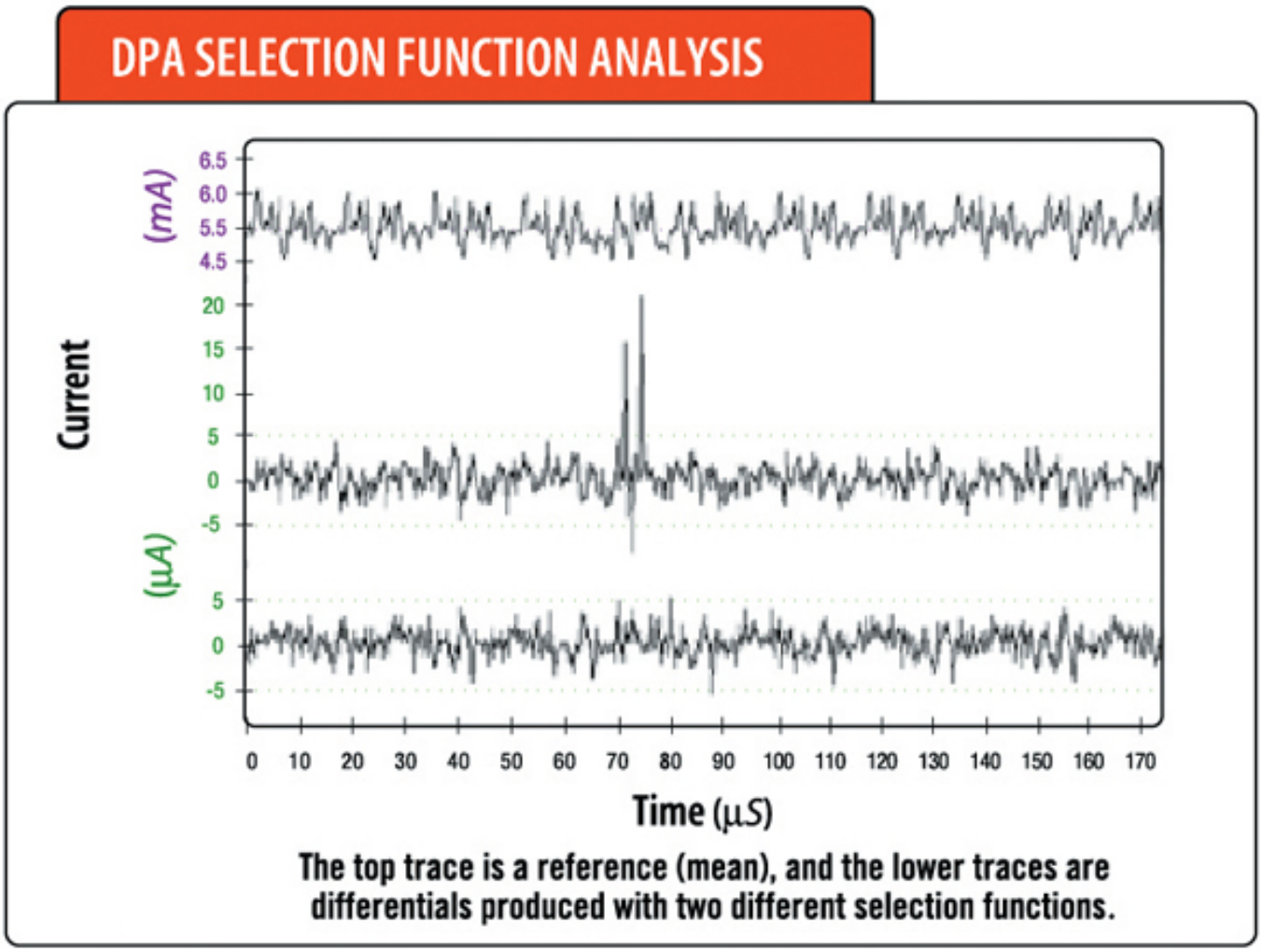
Protecting FPGAs from Power Analysis

Pankaj Rohatgi, Cryptography Research

 The advantages of FPGAs include reduced time-to-market, field-reconfigurability, and lower up-front costs. These benefits, together with recent gains in size and performance, make FPGAs ideally suited for many commercial and government applications. For sensitive defense systems, FPGAs may also be selected to help mitigate threats from hardware-based Trojans introduced during the ASIC manufacturing process. As a result, FPGAs are increasingly being relied upon to protect highly-sensitive intellectual property, trade-secrets, algorithms, and cryptographic keys.

Sensitive FPGA applications require strong tamper resistance to protect both the secrets contained within these devices as well as the data they process. Power analysis attacks are among the most important to protect against, since these attacks are non-invasive, widely understood by adversaries, and easy to mount using off-the-shelf oscilloscopes.

To mount a power analysis attack, an attacker passively measures the power consumption or electromagnetic emissions of a device containing an FPGA. The resulting measurements will reveal aggregated and noisy information related to the sensitive data being processed by the device. Simple power analysis (SPA) and differential power analysis (DPA) attacks utilize this information to recover secrets from the device. SPA uses direct observation of features within individual power consumption measurements, whereas DPA employs statistical techniques across multiple measurements to extract secrets. If a design does not have adequate countermeasures, sensitive information such as IP, trade-secrets and cryptographic keys can be extracted, and adversaries can make unauthorized modifications to the device configuration.



There are many published works reporting specific SPA and DPA vulnerabilities found in FPGA-based implementations of popular cryptographic algorithms, including RSA, ECC, AES and DES/3DES. While FPGAs differ somewhat from software implementations in how they leak information, the basic principles of SPA and DPA apply equally well to software, FPGAs, and ASICs.

The flexibility of FPGAs makes them a preferred platform for researchers investigating power analysis vulnerabilities and countermeasures. The National Institute of Advanced Industrial Science and Technology (AIST) of Japan has produced a series of FPGA-based Side-channel Attack Standard Evaluation Board (SASEBO) designs, which have become a standardized platform for such research. For example, we recently demonstrated a DPA attack that collects all the necessary data and extracts the full 128-bit key from a typical FPGA AES implementation, all in less than 2 minutes.

SPA and DPA vulnerabilities in FPGAs are not just limited to algorithms implemented within the fabric. Many FPGAs include microprocessors, math blocks and security features such as bitstream decryption, password protection, key storage, etc. In the absence of effective power analysis countermeasures, these platform level components and protections will be vulnerable to side-channel attacks.

For designers, the good news is that SPA and DPA are not new threats. Effective,

field-tested countermeasures are known and widely deployed to protect hardware devices used in other high-threat, but cost-sensitive, environments. For example, billions of security ICs, manufactured each year for the financial and content protection industries, contain highly effective countermeasures to SPA/DPA licensed from Cryptography Research, which owns the fundamental IP in this space. The same kinds of countermeasures are increasingly being licensed for securing FPGA implementations.

These countermeasure strategies include techniques to minimize information leakage, introducing noise to drown out leakage signals, use of randomness to mask computational intermediates, algorithm and implementation obfuscation and the use of protocols designed to preserve secrecy even in the presence of some leakage. Implementing countermeasures in FPGAs is also easier compared to ASICs, since designers can iteratively refine and test their implementations till the desired level of DPA-resistance is achieved.