

For additional information on Cryptography Research:

Patrick Corman
Corman Communications
(650) 326-9648
Patrick@cormancom.com

David Finkelstein
Corman Communications
(917) 523-1161
david@cormancom.com

FOR IMMEDIATE RELEASE

Cryptography Research Introduces Tool to Help Make Smart Cards Safer

New DPA Workstation Cuts Time, Cost to Test for Smart Card Leaks

SAN FRANCISCO, Calif., December 2, 2002 -- A Differential Power Analysis workstation introduced today by Cryptography Research, Inc. promises to make smart cards safer by reducing the time and cost required for testing power-related security vulnerabilities. The Cryptography Research DPA Workstation makes it easier and less costly for smart card manufacturers, testing labs and academic researchers to evaluate implementations and improve resistance to DPA attacks in smart cards and other tamper-resistant devices.

Differential Power Analysis enables an intruder to extract secret keys and information from smart cards and secure cryptographic tokens, which can be used to create fraudulent transactions, generate counterfeit digital cash or perform content piracy. DPA eavesdrops on the fluctuating electrical power consumption of the microprocessors at the heart of these devices, and uses advanced statistical methods to extract cryptographic keys and other secrets. Although DPA attacks currently require a high level of technical skill in several fields to implement, they can be repeated using a few thousand dollars worth of standard equipment, and can often break a device in a few minutes. DPA and related attacks were discovered at Cryptography Research by researchers Paul Kocher, Joshua Jaffe and Benjamin Jun.

"To be secure, smart cards have to be resistant to Differential Power Analysis, but equipment for testing for the problem hasn't been available," said Paul Kocher, president of

Cryptography Research. "The DPA Workstation offers vendors the first off-the-shelf tool for studying products' power analysis vulnerabilities and testing countermeasures."

Smart cards are already in widespread use in Europe and Asia, and are now gaining in popularity in the U.S. and Canada. According to the Smart Card Alliance, over 31 million smart cards shipped for use in the U.S. and Canada in the first half of 2002, doubling from the same period in 2001. Besides providing more protection for credit card, stored value and pay television systems, smart cards are finding increasing application in a variety of security and identity-related functions by business and government.

"The discovery of Differential Power Analysis was a brilliant end-run attack on many implementations of seemingly invincible cryptosystems," said Dr. Martin Hellman, Professor Emeritus of Electrical Engineering at Stanford University and co-inventor of public-key cryptography. "The Cryptography Research platform enables researchers to study information leakage in actual silicon, and provides an invaluable tool for improving the security of smart cards and related hardware."

Cryptography Research has been awarded a portfolio of fundamental patents covering countermeasures to DPA attacks, including U.S. patents #6,381,699; #6,298,442; #6,327,661; #6,278,783; #6,304,658; and others pending. The company hopes that availability of the DPA Workstation will help licensees improve their use of licensed countermeasures, while helping unlicensed vendors recognize the need to obtain licenses and improve their products.

Availability

The Cryptography Research DPA Workstation combines a high-end PC, analysis software, digital sampling equipment and custom test fixture. For security reasons, the product is sold directly from CRI and is only available to legitimate qualified research institutions, testing labs and product manufacturers. The workstation is available now.

About Cryptography Research, Inc.

Cryptography Research, Inc. provides consulting services and technology to solve complex security problems. In addition to security evaluation and applied engineering work, CRI is actively involved in long-term research in areas including tamper resistance, content protection, network security, and financial services. This year, security systems designed by

Cryptography Research engineers will protect more than \$40 billion of commerce for wireless, telecommunications, financial, digital television, and Internet industries. For additional information or to arrange a consultation with a member of the technical staff, please contact Jennifer Craft at 415-397-0329 or visit www.cryptography.com.

#