



December 19, 2011

Cryptography Research and INVIA SAS Sign Developer Agreement for Differential Power Analysis Countermeasures

Agreement enhances ASIC and FPGA security for subscriber identification modules, smart cards, PayTV, Secure ID, digital rights management, as well as military and defense applications

SAN FRANCISCO & MEYREUIL, France--(BUSINESS WIRE)-- Cryptography Research, Inc. (CRI), a division of [Rambus](#) (NASDAQ:RMBS), and INVIA SAS (INVIA) today announced they have entered into an agreement enabling INVIA to develop products incorporating Differential Power Analysis (DPA) countermeasures for use by licensees of CRI's DPA patents. INVIA provides security-related semiconductor design IP and embedded software to ASIC and FPGA designers.

"As part of our focus on delivering high-quality, tamper-resistant security blocks to our ASIC and FPGA customers, we are pleased to join the Cryptography Research DPA countermeasures developer ecosystem," said Robert Leydier, INVIA's president. "Working with CRI further strengthens the protection from major security threats we offer our semiconductor customers."

DPA is a form of attack that involves monitoring the fluctuating electrical power consumption of a target device and then using advanced statistical methods to derive cryptographic keys and other secrets. Strong countermeasures to DPA help protect tamper-resistant products used in applications such as military and aerospace products, smartphones and other mobile applications, banking, pay television, mass transit, secure ID, secure storage, automobiles and consumer electronics.

"DPA countermeasures are a crucial component of secure systems," said Pankaj Rohatgi, technical director, Hardware Security Solutions at Cryptography Research. "INVIA has developed DPA-resistant hardware cores tailored to address the anti-tamper needs of our licensees, and we are pleased to have INVIA join our DPA countermeasures ecosystem."

Cryptography Research has been awarded a portfolio of over 55 patents covering countermeasures to DPA attacks, with additional patent applications pending worldwide. For additional information about CRI or the DPA Workstation™ platform visit www.cryptography.com.

About Cryptography Research, Inc.

Cryptography Research, Inc. (CRI), a division of Rambus Inc., is a leader in semiconductor security research and development. Established by internationally renowned cryptographer Paul Kocher, CRI develops and licenses innovative technologies in areas including tamper resistance, content protection, anti-counterfeiting, network security, and financial services. Over five billion security products are made each year under license from CRI. Security systems designed by CRI scientists and engineers protect hundreds of billions of dollars in commerce annually. Additional information is available at www.cryptography.com.

About Rambus Inc.

Rambus is one of the world's premier technology licensing companies. Founded in 1990, the Company specializes in the invention and design of architectures focused on enriching the end-user experience of electronic systems. Rambus' patented innovations and breakthrough technologies help industry-leading companies bring superior products to market. Rambus licenses both its world-class patent portfolio, as well as its family of leadership and industry-standard solutions. Headquartered in Sunnyvale, California, Rambus has regional offices in North Carolina, Ohio, India, Germany, Japan, Korea, and Taiwan. Additional information is available at www.rambus.com.

About INVIA

INVIA is a privately held company founded in 2006 by smart card industry veterans. INVIA provides security related design IP to ASIC & FPGA designers. INVIA products protect silicon designs against tampering, reverse engineering, cloning and other major security threats. INVIA also provides embedded software cryptography for ARM Cortex and SPARC processors. INVIA's IPs are used in millions of field-proven devices. Our R&D's experience in secure hardware and software exceeds 150 men years and is protected by a patent portfolio.

EUROPE

Andrew Lloyd & Associates

Carol Leslie, +44 1273 675100

carol@ala.com

or

UNITED STATES

Schwartz Communications

Samantha Sok, +1-415-817-2549

ssok@schwartzcomm.com

Source: Cryptography Research, Inc.

News Provided by Acquire Media