



December 19, 2012

Cryptography Research Announces Riscure as an Accredited Evaluation Lab for DPA Testing Program

Security research firm now certified to independently test SoCs and FPGAs to validate security of chips used in set-top boxes, game consoles, and mobile devices

SAN FRANCISCO & DELFT, Netherlands--(BUSINESS WIRE)-- Cryptography Research (CRI), a division of Rambus Inc. (NASDAQ:RMBS), today announced the accreditation of Riscure as an independent testing lab to conduct evaluations for the Differential Power Analysis (DPA) Countermeasure Validation Program. The program specifies procedures for rigorous independent testing of products to evaluate their resistance to DPA and related side channel attacks to help chip purchasers and downstream customers identify devices with the most effective security.

Cryptography Research accredited Riscure because of its expertise in testing complex devices for security against DPA and side channel attacks.

"Protection against DPA is increasingly critical for a broad spectrum of SoCs and devices," said Pascal van Gimst, director sales and business development of Riscure. "We're pleased to be a part of CRI's DPA Countermeasure Validation Program, which is crucial in helping our customers understand and ensure security at both the hardware and software layers of set-top boxes, game consoles, mobile phones, tablets and other devices."

Riscure, with offices located in San Francisco and the Netherlands, joins Brightsight BV in the Netherlands, Thales CEACI in France, and T-Systems in Germany, as the fourth security evaluation facility accredited to conduct testing under the DPA Countermeasure Validation Program. Products that pass the rigorous testing conducted by accredited labs become eligible to carry the "DPA Lock" certification symbol.

"CRI is pleased to announce Riscure as an accredited laboratory under the DPA Countermeasure Validation Program," said Pankaj Rohatgi, technical director, Hardware Security Solutions of CRI. "This accreditation reflects Riscure's extensive expertise in security testing, including side-channel analysis of smart card ICs, pay television SoCs, FPGAs, and other devices."

Differential power analysis attacks extract secret keys by analyzing measurements in the power consumption of a target device. Cryptography Research licenses DPA countermeasure technologies to a broad spectrum of chip and product vendors, included in over 6 billion devices a year. The DPA Countermeasure Validation Program specifies a suite of tests to verify the effectiveness of a device's countermeasures against power analysis attacks.

To learn more about Cryptography Research of the DPA Countermeasures Validation Program, visit www.cryptography.com.

RMBSTN

About Riscure

Riscure is a globally recognized and independent security test laboratory. Riscure is specialized in evaluating and testing the security of smart cards and embedded devices that are designed to operate securely in any environment and under all circumstances. Riscure offers these services in different markets such as payment, conditional access, telecom and automotive. Besides that, Riscure develops and maintains security test tools. Inspector, Riscure's side channel analysis and fault injection test tool is used by manufacturers and research labs to evaluate the resistance of chips against high attack potential. Additional information is available at www.riscure.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 six 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 an innovative solutions company that brings invention to market. Unleashing the intellectual power of our world-class engineers and scientists in a collaborative and synergistic way, Rambus invents, licenses and develops solutions that challenge and enable our customers to create the future. While best known for creating unsurpassed semiconductor memory architectures, Rambus is also developing world-changing products and services in security, advanced LED lighting and displays, and immersive mobile media. Additional information is available at www.rambus.com.

RMBSTN

CRI

EUROPE

Andrew Lloyd & Associates

Carol Leslie, +44 1273 675100

carol@ala.com

or

UNITED STATES

Schwartz Communications

Dan O'Mahony, 415-512-0770

cri@schwartzmsl.com

or

RISCURE

Europe

Pascal van Gimst, +31 15 251 4090

Director Sales & Business Development

vangimst@riscure.com

or

United States

Jasper van Woudenberg, 650-646 9979

CTO Riscure North America

vanwoudenberg@na.riscure.com

Source: Cryptography Research, Inc.

News Provided by Acquire Media