February 4, 2015

MStar to Use Cryptography Research DPA Countermeasures to Ward Off Attacks in Set-Top Box Solutions

Added security technologies protect tamper-resistant chips in digital home market

SUNNYVALE, Calif. & TAIPEI, Taiwan--(BUSINESS WIRE)-- Rambus Inc. (NASDAQ:RMBS) today announced that its Cryptography Research Division and MStar, a leading global semiconductor company for display and digital home solutions, have signed a license agreement for the inclusion of advanced DPA countermeasure technologies developed by Cryptography Research in MStar products. By incorporating these patented technologies, MStar's tamper-resistant products, including set-top box chipsets, can be protected against differential power analysis (DPA) and related attacks.

"With growing threats impacting the content distribution market, we are committed to providing the highest level of security for our customers," said Jeff Wu, Associate VP at MStar. "DPA countermeasures are integral to providing the highest level of security and now our solutions incorporate comprehensive security ingredients to protect against side-channel and other non-invasive attacks."

DPA is a form of side-channel attack that involves monitoring the fluctuating electrical power consumption or EM emissions from a target device and then using advanced statistical methods to derive cryptographic keys and other secrets from chips. Since these types of attacks can affect set-top boxes and other consumer electronic devices, there is a growing need in the entertainment industry for advanced side-channel attack solutions to provide secure delivery of high quality content to homes.

"As it becomes easier to mount attacks using DPA, content distributors need protection against side-channel attacks to satisfy requirements in order to provide secure access to high value content," said Paul Kocher, president and chief scientist of the Rambus Cryptography Research division. "By incorporating DPA countermeasures into their set-top box chipsets, MStar is demonstrating their commitment to deploying comprehensive security measures in the pay TV space."

Cryptography Research DPA countermeasure technologies are designed to protect devices against certain types of attacks that can extract cryptographic keys and other sensitive data from chips in set-top boxes and other home networking products. By integrating more comprehensive security solutions into set-top boxes, unauthorized access of premium content can be prevented.

About Cryptography Research

The Rambus Cryptography Research division specializes in embedded security solutions to combat the worldwide threat to data integrity, our innovative technologies span areas including tamper resistance, content protection, network security, media and payment and transaction services. Eight billion security products are made annually with our security technology, and systems designed by our scientists and engineers protect hundreds of billions of dollars in revenues every year. Additional information is available at cryptography.com.

About MStar Semiconductor, Inc.

MStar Semiconductor, Inc. is a world-class leader in Application Specific ICs with a focus on consumer electronic products and communication applications. Since the inception in 2002, MStar has established a strong brand and leadership position in LCD controller, analog and digital TV, and set-top box by fully leveraging its core expertise of cutting-edge design capabilities, continuous innovation and premier customer-focused services. Headquartered in Taiwan, MStar has a comprehensive global footprint of international R&D and customer support centers to provide a full range of total solutions for various consumer electronic applications. For more information, please visit www.mstarsemi.com.

RMBSTN

Cryptography Research
MSLGROUP
Sam Katzen, 415-512-0770
rambus@mslgroup.com

Source: Rambus Inc.