

# CHES2009 RUMP SESSION

Bart Preneel

"The International Association for Cryptologic Research (IACR)"

Ilya Kizhvatov

"On Physical Insecurity of Some Embedded Devices"

Jean-Philippe Aumasson

"Zero-sum distinguishers"

Marc Witteman

"Elastic Alignment"

Christophe Giraud & Hugues Thiebauld

"The Power Attacks Glossary"

Werner Schindler

"COSADE 2010"

Daniel J. Bernstein, Hsueh-Chung Chen, Ming-Shing Chen, Chen-Mou Cheng, Chun-Hung Hsiao, Tanja Lange, Zong-Cing Lin, and Bo-Yin Yang

"The Billion-mulmods-per-second PC"

Alessandro Barenghi, Guido Bertoni, Marco Macchetti, Francesco Ragazzoni

"DPA attack to devices up to billion gates"

Josh Jaffe

"A chosen message DPA attack on MISTY1"

Daniel J. Bernstein

"binary.cr.yip.to"

Tanja Lange

"The ECC challenge"

Amir Moradi

"A Really True Random Number Generator "

Takeshi Shimoyama

"How do you feel in the Cover Picture of CHES?"

Johann Groszschädl

"Full Custom VLSI Design of a Low-Power Multiplier for ECC on RFID Tags"

Akashi Satoh

"Secrets of SASEBO"

Lejla Batina, Benedikt Gierlichs, Jorge Guajardo

"On the CHES Review Process - Some questions"