#	Authors	Title	Affiliation of Contact
1	Arash Hariri, Arash Reyhani-Masoleh	Fault Detection Structures for the Montgomery Multiplication over Binary Extension Fields	The University of Western Ontario, Canada
2	Frederic Amiel, Benoit Feix, Louis Marcel, Karine Villegas	Passive and Active Combined Attacks Combining Fault Attacks and Side Channel Analysis	Inside Contactless, France
3	Erdinc Ozturk, Gunnar Gaubatz, Berk Sunar	Tate Pairing with Strong Fault Resiliency	Worcester Polytechnic Institute, USA
4	Michael Tunstall	Montgomery Multiplication with Redundancy Check	University College Cork, Ireland
5	M. Mozaffari-Kermani, A. Reyhani-Masoleh	A Structure-independent Approach for Fault Detection Hardware Implementations of the Advanced Encryption Standard	The University of Western Ontario, Canada
6	Onur Acıicmez, Jean-Pierre Seifert	Cheap Hardware Parallelism Implies Cheap Security	Samsung Electronics R&D Center, USA
7	P. Maistri, P. Vanhauwaert, R. Leveugle	A Novel Double-Data-Rate AES Architecture Resistant against Fault Injection	TIMA Laboratory, France
8	G. Agosta, L. Breveglieri, I. Koren, G. Pelosi, M. Sykora	Countermeasures Against Branch Target Buffer Attacks	Politecnico di Milano, Italy
9	Junko Takahashi, Toshinori Fukunaga, Kimihiro Yamakoshi	DFA Mechanism on the AES Key Schedule	Nippon Telegraph and Telephone Corporation, Japan

#	Authors	Title	Affiliation of Contact
10	Richard Stern, Nikhil Joshi, Kaijie Wu, Ramesh Karri	Register Transfer Level Concurrent Error Detection in Elliptic Curve Crypto Implementations	Polytechnic University Brooklyn, USA
11	Chong Hee Kim, Jean-Jacques Quisquater	How can we overcome both Side Channel Analysis and Fault Attacks on RSA-CRT ?	Université Catholique de Louvain, Belgium
12	Helena Handshuh, Elena Trichina	Securing Flash Technology	Spansion, USA
13	Odile Derouet	Secure Smartcard Design against Laser Fault Injection Attacks	Samsung, Korea