rcd 2017

romanian
cryptology
days

AGENDA

SERVICIUL DE INFORMAŢII EXTERNE ROMÂNIA

September 18-20, 2017
Bucharest, ROMANIA

Romanian Academy Library

http://www.sie.ro/rcd2017

ACADEMIA ROMANA

Monday, September 18th, 2017

09:00 – 09.50	**Registration and Welcome coffee**	
10:00 – 11:15	**Session 1.**	
	Opening Remarks	**Liet. Gen. Vasilică Sarcă** – Deputy Director FIS
		Acad. Ionel-Valentin Vlad – President of Romanian Academy
	Vincent Rijmen – *Galileo Navigation Message Authentication (60')*	
11:15– 11:30	**Coffee Break**	
11:30 – 13:30	**Session 2. Chair: Vincent Rijmen**	
	Ingrid Verbauwhede – *Implementation aspects of post-quantum crypto in embedded devices (60')*	
	Eli Biham – *Conditional Linear Cryptanalysis (60')*	
13:30 – 14:30	**Lunch**	
14:30 – 16:30	**Session 3. Chair: Ingrid Verbauwhede**	
	Ahmad-Reza Sadeghi – *Hardware-Assisted Security: Promises, Pitfalls and Opportunities (60')*	
	Marc Stevens – *The first collision for full SHA-1 (45')*	
	Kay Lukas – *Cube attacks on PRIMATEs (Paper) (15')*	
16:30 – 17:00	**Coffee Break**	
17:00 – 18:30	**Session 4. Chair: Ferucio-Laurențiu Țiplea**	
	Ioana Boureanu – *How (not) to use TLS between 3 parties (45')*	
	Tania Richmond – *The simple roots problem (Paper) (15')*	
	Ruxandra Olimid – *On low-cost privacy exposure attacks in LTE mobile communication (Paper) (15')*	
	Andrei Ene – *Privacy preserving vector quantization Based Speaker Recognition System (Paper) (15')*	

Tuesday, September 19th, 2017

08:30 – 09:00	**Coffee Break**
09:00 – 11:00	**Session 5. Chair: Bart Preneel**
	Joan Daemen – *Column-parity mixing layers (60’)*
	Lejla Batina – *Side-channel attacks on ECC: an overview (45’)*
	Raluca Posteucă – *New related-key attacks and properties of SKINNY-64-128 cipher (Paper) (15’)*
11:00 – 11:15	**Coffee Break**
11:15 – 13:30	**Session 6. Chair: Eli Biham**
	Bart Preneel – *Cryptocurrencies and Blockchain (60’)*
	Bogdan Warinschi – *Cryptographic building blocks for electronic voting (60’)*
	Adrián Ranea – *An Easy-to-use tool for rotational-XOR Cryptanalysis of ARX Block Ciphers (Paper) (15’)*
13:30 – 14:30	**Lunch**
14:30 – 16:00	**Session 7. Chair: Joan Daemen**
	Cristian Calude – *A Quantum Random Generator Certified by KOCHEN-Specker Theorem (60’)*
	Emil Simion – *New results concerning the power of NIST randomness tests (Paper) (15’)*
	Tudor Patuleanu – *True random number sequences from gamma-decay using four extraction methods (Paper) (15’)*
16:00 – 16:30	**Coffee Break**
16:30 – 18:00	**Session 8. Chair: Adriana Vlad**
	Ferucio-Laurențiu Țiplea – *Unpredictability of Jacobi Sequences (45’)*
	Daniel Plecan – *Cryptographic access control for mandatory security policies using attribute-based encryption (Paper) (15’)*
	Adrian Diaconu – *Correlation distribution of adjacent pixels randomness test for image encryption (Paper) (15’)*
	Mihai Togan – *On DHCP Security (Paper) (15’)*
18:00 – 18:30	**Closing remarks and Cocktail**

Wednesday, September 20th, 2017

Workshop - Cybersecurity in a Post-quantum World

08:30 – 09:00	**Coffee Break**
09:00 – 11:00	**Session 1.**
	Yuval Elovici – *Emergence on Cyber-Security Challenges (60')*
	Stig Mjølsnes – *IMSI-catchers and mobile privacy protocols (60')*
11:00 – 11:30	**Coffee Break**
11:30 – 13:30	**Session 2.**
	Joppe Bos – *Post-Quantum Key Exchange based on Lattices (60')*
	Virgil Gligor – *Establishing Secure System States Unconditionally (60')*
13:30 – 14:30	**Lunch**
14:30 – 16:30	**Session 3.**
	Gregor Leander – *Quantum Attacks on Symmetric Crypto (60')*
	Viktor Galliard – *TBA (60')*
16:30 – 17:00	**Coffee Break**
17:00 – 18:00	**Session 4.**
	Jeremiah Spradlin – *What scares me today: an industry perspective on the arrival of post-quantum (60')*