

Table of Contents

Efficient Implementations and designs

A Lightweight ATmega-Based Application-Specific Instruction-Set Processor for Elliptic Curve Cryptography	1
<i>Erich Wenger</i>	
ITUbee: A Software Oriented Lightweight Block Cipher	16
<i>Ferhat Karakoç, Hüseyin Demirci, and A. Emre Harmancı</i>	

Block Cipher Cryptanalysis

Related-Key Slide Attacks on Block Ciphers with Secret Components ...	28
<i>Meltem Sönmez Turan</i>	
Differential Fault Attack on the PRINCE Block Cipher	43
<i>Ling Song and Lei Hu</i>	
Multidimensional Meet-in-the-Middle Attacks on Reduced-Round TWINE-128	55
<i>Özkan Boztaş, Ferhat Karakoç, and Mustafa Çoban</i>	

Wireless Sensor Networks

An Implementation of the Hash-Chain Signature Scheme for Wireless Sensor Networks	68
<i>Nadia Mourier, Reinhard Stampf, and Falko Strenzke</i>	
An Adaptive Security Architecture for Location Privacy Sensitive Sensor Network Applications	81
<i>Jiří Kůr and Václav Matyáš</i>	

Cryptographic Protocols

Secure and Lightweight Distance-Bounding	97
<i>Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay</i>	
Cryptanalysis and Improvement of a Provably Secure RFID Ownership Transfer Protocol	114
<i>Daisuke Moriyama</i>	

An Efficient and Private RFID Authentication Protocol Supporting
Ownership Transfer 130
 Süleyman Kardaş, Serkan Çelik, Atakan Arslan, and Albert Levi

Author Index 143