Security In Embedded Devices

DOWNLOAD HERE

Implementation;127 1.7.2.2;6.2.2 CAST;128 1.7.2.3;6.2.3 TEA;130 1.7.2.4;6.2.4 HIGHT;131 1.7.2.5;6.2.5 PRESENT Cipher;133 1.7.3;6.3 Stream Ciphers;134 1.7.3.1;6.3.1 Stream Cipher Principles;135 1.7.3.2;6.3.2 RC4;137 1.7.3.3;6.3.3 Grain;138 1.7.4;6.4 Cipher Modes of Operation;139 1.7.5;6.5 Authenticated Modes for Encryption;142 1.7.6;6.6 Embedded Systems Implications;144 1.7.7;References;147 1.8;7 Data Integrity and Message Authentication;149 1.8.1;7.1 Properties of Hash and MAC;151 1.8.2;7.2 The Structure of Integrity and Authentication Functions;154 1.8.2.1;7.2.1 The SHA-2 Function;158 1.8.3;7.3 Integrity Trees;160 1.8.4;7.4 Embedded Implications;163 1.8.5;References;166 1.9;8 Side Channel Attacks on the Embedded System;168 1.9.1;8.1 The Side Channel;168 1.9.1.1;8.1.1 Theory of the Side Channel;169 1.9.1.2;8.1.2 The Side Channel Attack in Practice;171 1.9.1.2.1;8.1.2.1 EM Probe;173 1.9.1.2.2;8.1.2.2 The Oscilloscope;176 1.9.1.2.3;8.1.2.3 Device and Trigger;178 1.9.1.3;8.1.3 Setting up a SCA;179 1.9.2;8.2 What is Simple Analysis;181 1.9.3;8.3 Differential Analysis;184 1.9.4;8.4 Correlation Analysis;194 1.9.5;8.5 Differential Frequency Analysis;195 1.9.6;8.6 Experiments on PDAs;196 1.9.6.1;8.6.1 EM Results;200 1.9.6.1.1;8.6.1.1 SEMA of AES on the PDA;202 1.9.6.1.2;8.6.1.2 Truncated code Analysis of the PDA;208 1.9.6.1.3;8.6.1.3 Attack of the Device Using Full AES;214 1.9.7;8.7 Experiment EAN/ISBN : 9781441915306 Publisher(s): Springer, Berlin, Springer US Format: ePub/PDF Author(s): Gebotys, Catherine H.