Structure:

1 Historic development of Cryptographic Chips: From Enigma to Ecolex and AroFlex 13

2 Transformation of Cryptography influences Secure Embedded Systems in a Network 15

3 The Echo Protocol: Networking Encrypting Devices 21

4 Hardware Architecture 27

4.1 Cryptographic Conversions on Secure Embedded Systems 30
4.2 Example: NitroKey 32
4.3 Example: Arduino & Raspberry Pi 34
4.4 Defining the architectural Design of Echo on a Chip (EoC) 35

5 Hardware Echo-Chip - Part # I - Encryption and Decryption Processes on a Trusted Execution Environment 41

5.1 Communication Methods Zone: TCP-Disconnected Communication Methods via Protocol-Change, e.g. Bluetooth or UDP 42
5.2 McEliece Key & Algorithm Zone 43
5.3 Public Key Infrastructure Zone for Decryption & Encryption 48

Bibliografische Informationen
https://d-nb.info/1208558323

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

5.4 Cascading / Multi-Encryption 48
5.5 Local Private Application Interfaces 49

6 Hardware Echo-Chip - Part # II - Meshing the Flood: Implementing Routing and Graph Theory into Hardware 52

6.1 Congestion Control Zone 52
6.2 Local Broadcast Manager & Listener Broadcasting Zone 53
6.3 Neighbors Zone 54

7 Hardware Echo-Chip - Part # III - Key Servers & Ozone Postbox Functionalities 55

7.1 Congestion Control Zone 55
7.2 Database or Memory Containers Zone 55
7.3 Neighbors Zone 56
7.4 Discovery via Cryptography 56
7.5 Ozone Address / PostBox Zone 57
7.6 Private Public-Key Server & Private Servers Zone 58

8 Conclusions for contextual risk cases with research and development requirements 61

8.1 Risk Case: From ToTok to TikTok 61
8.2 Risk Case: Android @ Huawei 65
8.3 Risk Case: Virus-Scanner Kasperspky et al. 67
8.4 Risk Case: BIOS Firmware 72
8.5 Risk Case: 5G Telecommunication-Chips 76
8.6 Risk Case: Closed Source Operating System Windows 80
8.7 Risk Case: Closed Internet Networks like #RUNET 83

9 The Secure Architecture Model (SAM) extends and integrates the OSI-Model 85

10 Literature 97

11 Didactical Questions 108