Echo on a Chip

**A New Perception for the
Next Generation of Micro-Controllers
handling Multi-Encryption for Mobile Messaging**

From Secure Embedded Systems to
Separated Secure Embedded Systems (SSES)
in Cryptography

Hardware supported
Trusted Execution Environments (TEE)

Mancy A. Wake
Dorothy Hibernack
Lucas Lullaby

Structure:

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

2. ***Transformation of Cryptography influences Secure Embedded Systems in a Network***

3. ***The Echo Protocol: Networking Encrypting Devices***

4. ***Hardware Architecture***
    - 4.1 Cryptographic Conversions on Secure Embedded Systems
    - 4.2 Example: NitroKey
    - 4.3 Example: Arduino & Raspberry Pi
    - 4.4 Defining the architectural Design of Echo on a Chip (EoC)

5. ***Hardware Echo-Chip - Part # I - Encryption and Decryption Processes on a Trusted Execution Environment***
    - 5.1 Communication Methods Zone: TCP-Disconnected Communication Methods via Protocol-Change, e.g. Bluetooth or UDP
    - 5.2 McEliece Key & Algorithm Zone
    - 5.3 Public Key Infrastructure Zone for Decryption & Encryption
    - 5.4 Cascading / Multi-Encryption
    - 5.5 Local Private Application Interfaces

10. ***Literature***

11. ***Didactical Questions***

ABSTRACT: Going the Extra Mile - Security through Separation

Based on the historical development of so-called Crypto-Chips, the current transformation of cryptography shows numerous changes, innovations and new process designs in the field of cryptography, which also need to be integrated in a hardware design of microprocessors and microcontrollers for a secure embedded system.

Single-board computers like Raspberry Pi or Arduino and also devices with cryptographic functions such as the NitroKey and others allow developers to create their design architectures accordingly.

Using the example of the encrypting Echo protocol, a design of a hardware architecture based on three chips with cryptographic functions corresponding to the protocol is described.

The central echo chip # 1 represents a "Trusted Execution Environment" (TEE), which is not connected to the Internet for the conversion processes from plaintext to ciphertext and is supposed to remain quasi original, to prevent software injections or possible uploads of copies of the plaintext.

The export and transport of the encrypted Echo capsules can then be regulated using other ways, methods and protocols than TCP. The same applies to deciphering the packets to be delivered.

The two other chips then take over predominantly routing, respective forwarding and further server functions.

The technical specifications of the three microprocessors for the individual functions of Echo and encryption are described in detail.

The established paradigm of separation is recognized as a security feature and discussed as a perception for a next generation of micro-controllers in the field of mobile messaging under the technical term "Going the Extra Mile". Going the Extra Mile means using your own platform or hardware that is separate from the network for the conversion from plaintext to ciphertext and vice versa.

This security architecture is then discussed in the context of seven different current risk cases with the consolidated result that the well-known OSI (Open Systems Interconnection) model can be expanded to a thirteen-stage model: This essay introduces the basis of the Secure Architecture Model, abbreviated SAM, that integrates the previous OSI model and builds on it to examine the further effects and further research needs for a department of cryptography and its related disciplines, in particular the Secure Embedded Systems and as well other areas.

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

In the past, cryptographic micro-controllers had primarily these functions since their first development in the mid-1970s (e.g. by Philips Usfa Crypto) - roughly in line with the spread of asymmetric encryption of a public key infrastructure (PKI):

- to carry out the encryption with the aid of a computer with a dedicated computing machine
- to offer the process to dedicated customers such as military or individual governments
- to convert ciphertext faster or more adapted to possibly more complex algorithms of the respective era
- respective to relate it in particular to the encryption of speech
- or to operate different channels in parallel –
- and above all: to include an uninfluenced, hardware-supported number generator.

Previously, the development of the Crypto-Chips was based on symmetrical encryption, just as Philips started with a one-time tape (OTT) called ECOLEX in 1956 (Philips Usfa 1982).

The Crypto-Chips digitized the previously mechanical encryption processes in an electronic processor, e.g. of the Enigma machines that have been developed by Chiffriermaschinen AG since the mid-1920s.

In the architectures, several chips were often chained one after the other in order to map cryptographic routines, for example to implement a stream cipher: Eight such chips were e.g. connected in the AroFlex machine. They were also called "crypto hearts" (Kraan 1986).

Likewise, a lot has been technically adapted over the years to make the chips more contemporary in their hardware, for example in the case of the transistors, or to adapt them to the general chip development. Today, single-board computers such as Raspberry Pi or Arduino and others are available and programmable for everyone.

The security of the uses of these “embedded systems” remains to be assessed and designed according to modern processes and standards of cryptography.

Other crypto machines that also used microprocessors, such as those from Crypto AG, were manipulated.

The Secret Service Coup of the Century first went public in 2020: The CIA and the German BND had bought the Swiss Crypto AG in 1970 under cover behind trustees. The hardware produced had been manipulated in order to be able to intercept governments from more than 100 countries that were customers of Crypto AG (Miller et al. 2020).

Hence, the development of secure embedded systems remains a hot topic for cryptography in the face of these disclosed historical developments.

2 Transformation of Cryptography influences Secure Embedded Systems in a Network

The more recent developments in cryptography in the 21st century are not only one-sided towards future quantum cryptography (PQCrypto 2019, Zimmermann 2019), but are already showing today fundamental changes in numerous existing processes:

It starts with multi-encryption, goes via Instant Perfect Forward Secrecy (IPFS) with end-to-end encryption with Cryptographic Calling, the adaptation of cryptographic protocols as through Fiasco Forwarding, in which up to a dozen keys out of a pool are used to decode a message.

It continues to solve the key transport problem with Secret Streams and Juggerknaut keys to a volatile and Exponential Encryption.

In their book "Transformation of Cryptography", the authors Linda Bertram and Gunther van Dooble (2019) have, for example, compiled over two dozen of these changes and innovative concepts that are currently influencing cryptography and whose transformation characterizes them: One can currently speak of a “Transformation of Cryptography”.

The transformation is therefore not just about the step into cryptography that is resistant to the fast computing operations of quantum computers, for example by exchanging the RSA algorithm with algorithms such as NTRU or McEliece (ibid 1978), but also about numerous development steps, which are emerging in multiple, also process-oriented ways, such as multi-encryption and new Internet protocols such as the Echo protocol (Gasakis / Schmidt 2018), which combines multi-encryption with aspects of graph theory.