A Dedicated Hardware Security Module for Field Operational Tests of Car-to-X Communication

[Extended Abstract]

Attila Jaeger$^1$  
Hagen Stübing$^2$  
Sorin A. Huss$^1$

$^1$ Technische Universität Darmstadt, Integrated Circuits and Systems Lab  
Hochschulstraße 10, 64289 Darmstadt, Germany  
{jaeger, huss}@iss.tu-darmstadt.de

$^2$ Adam Opel AG, Advanced Engineering Active Safety  
Friedrich-Lutzmann-Ring, 65423 Rüsselsheim, Germany  
hagen.stuebing@de.opel.com

ABSTRACT

In this work a security module is developed, providing FPGA based hardware acceleration for Elliptic Curve Cryptography which meets the requirements of Car-to-X Communication. The module is pluggable via USB to a Car-to-X system and therefore easily deployable within currently running or planned Field Operational Tests.

Categories and Subject Descriptors

B.7 [Hardware]: Integrated Circuits

General Terms

Security, Performance

Keywords

Car-to-X, Security, ECC, ECDSA, ECIES, FPGA

1. INTRODUCTION

Intelligent Transportation Systems (ITS) based on Car-to-Car and Car-to-Infrastructure (Car-to-X, C2X) communication are considered to be one of the most promising attempts towards the improvement of active vehicle safety and traffic efficiency in the near future. However, Car-to-X communication systems are vulnerable to several attacks against security and drivers' privacy. The IEEE 1609.2 [1] standard proposes countermeasures by means of cryptographic techniques based on Elliptic Curve Cryptography (ECC). In this context, the standard specifies digital signatures according to ECDSA [2] to authenticate all exchanged C2X messages. To ensure confidentiality, the standard specifies optional encryption according to ECIES [3]. For both, signatures and encryption, a Public Key Infrastructure (PKI) for C2X communication has to be established to generate Public Key Certificates by Certificate Authorities (CAs).

However, computationally intensive operations on elliptic curves make it hard to achieve timing requirements on C2X architectures with hard limited computational resources. Therefore, e.g., in simTD, a largescale Field Operational Test (FOT) for Car-to-X in Germany [4], an adapted version of IEEE 1609.2 is deployed using RSA cryptography instead of ECC as further detailed in [5]. Providing comparable security levels, a RSA based approach leads to significant larger signatures and, thus, undesired increase of message sizes. Consequently, a dedicated security module including hardware acceleration for cryptographic primitives is needed to establish ECC in C2X.

In this work, a security implementation based on ECC is being developed which meets the requirements of Car-to-X FOTs. In particular, this requires a modular and adaptable design, which can be easily integrated into existing C2X architectures. As a nearseries implementation, it further has to be compliant to the IEEE 1609.2 standard.

2. ARCHITECTURE

The Security Module has to perform five major task: (1) Signing of outgoing messages with own identity certificates stored in a local certificate storage, (2) verifying incoming messages using the attached certificate, (3) encrypting outgoing messages with the receiver's public key, (4) decrypting incoming encrypted messages with own private key, and (5) verifying certificates attached to incoming messages by means of the respective CA certificate. Figure 1 shows the system architecture in terms of individual components and communication links between them. Since this paper describes ongoing work, not all parts of the module are finally implemented yet. In the schematic already implemented parts are drawn in solid lines, while not finished parts are denoted by dotted lines. However, meanwhile assembling components as shown in the architecture overview, also further modifications on already finished components might be necessary.

Messages are delivered serially via the USB Communication Interface. The control flow inside the Security Module is handled by a controller component. This module activates dedicated components for signing, verifying, encrypting, or decrypting and distributes the message via a local bus. The activated component has access to units for EC point multiplication ($k \cdot P$), inversion ($k^{-1}$), hashing (SHA), symmetric encryption (AES), and a random number generator (RNG).

For privacy reasons, used EC keys must be changed frequently. This way tracking is avoided. Consequently, a vehicle possesses multiple public/private key pairs with according certificates [5]. In case the local certificate pool will ex-
pire, a vehicle has to issue new keys and certificates. Therefore, the Security Module provides a component for generating public/private key pairs. Public keys are sent to a CA for certification while private keys never leave the vehicle. A permanent long term certificate is used to identify the station towards the CA. All tasks related to certificate management are handled by the Identity & Key Management.

For message signing and decryption, respective keys are loaded from local certificate storage. In case of sending an encrypted message or verifying a received message, an external key (and certificate) has to be loaded into the module.

We have chosen the BeMicro Evaluation Board [6], depicted in Figure 2, as target platform. Thus, the Security Module will be small, robust, and simple pluggable with USB to the Car-to-X system. In addition, although the components are optimized for this platform, the outcome of this work will be a fully synthesizable VHDL model which may be easily transferred to other target platforms, too.

The module is designed to relieve C2X system CPU, especially in FOTs. Therefore, we do not aim a high performance module, but one, which meets hard space requirements on the used FPGA with an acceptable timespace tradeoff. However, some preliminary evaluations on the chosen platform indicate that durations of about 15ms for signing and of about 30ms for verifying a signature using ECC with 224bit are reachable.

In our future work we further implement and refine our components.

4. REFERENCES


