Chapter 26
Elliptic Curve Cryptography on WISPs

Michael Hutter
Institute for Applied Information Processing and Communications, Graz University of Technology, Austria

Markus Pelnar
Institute for Applied Information Processing and Communications, Graz University of Technology, Austria

Erich Wenger
Institute for Applied Information Processing and Communications, Graz University of Technology, Austria

Christian Pendl
Institute for Applied Information Processing and Communications, Graz University of Technology, Austria

ABSTRACT

In this chapter, the authors explore the feasibility of Elliptic Curve Cryptography (ECC) on Wireless Identification and Sensing Platforms (WISPs). ECC is a public-key based cryptographic primitive that has been widely adopted in embedded systems and Wireless Sensor Networks (WSNs). In order to demonstrate the practicability of ECC on such platforms, the authors make use of the passively powered WISP4.1DL UHF tag from Intel Research Seattle. They implemented ECC over 192-bit prime fields and over 191-bit binary extension fields and performed a Montgomery ladder scalar multiplication on WISPs with and without a dedicated hardware multiplier. The investigations show that when running at a frequency of 6.7 MHz, WISP tags that do not support a hardware multiplier need 8.3 seconds and only 1.6 seconds when a hardware multiplier is supported. The binary-field implementation needs about 2 seconds without support of a hardware multiplier. For the WISP, ECC over prime fields provides best performance when a hardware multiplier is available; binary-field based implementations are recommended otherwise. The use of ECC on WISPs allows the realization of different public-key based protocols in order to provide various cryptographic services such as confidentiality, data integrity, non-repudiation, and authentication.

INTRODUCTION

Wireless Identification and Sensing Platforms (WISPs) are based on Radio Frequency Identification (RFID) technology. They provide the same capabilities as RFID tags but feature additional functionalities like sensing of data from the near proximity. Typical data that is collected by WISPs are the environmental temperature, light, or 3D acceleration of the device or of a targeted object. Among the most interesting features of WISPs is the possibility to perform customized operations using assembled microcontrollers. This allows individual handling of data collection, processing,

DOI: 10.4018/978-1-4666-2919-6.ch026

and monitoring of sensed information. However, for most of the applications, several security and privacy issues arise such as protecting sensitive data that have been collected by WISPs and that are transmitted over the air interface. This chapter addresses the implementation of Elliptic Curve Cryptography (ECC) on such platforms in order to overcome these concerns.

ECC is a public-key technique that has gained much importance especially in environments which provide only low resources. It features a high level of security while needing only small key sizes compared to other existing public-key techniques like RSA. There exist many ECC-based cryptographic protocols that have been standardized and evaluated over many years which encourage its use in security-related applications. The main operation in ECC is the scalar multiplication $Q = k \cdot P$ of a point P on an elliptic curve. This operation involves the group operations of addition and doubling of curve points which again are based on finite-field arithmetic. One of the most resource-consuming finite-field operations is the scalar multiplication which constitutes about 75% of the total runtime. Therefore, the performance of scalar multiplication largely determines the efficiency of ECC on WISPs. If the microcontroller which is assembled on the WISP provides a dedicated hardware multiplier, a word-size multiplication can be performed in a single clock cycle. If no hardware multiplier is supported, multiplication has to be implemented with the help of addition and shift operations which significantly reduce the overall performance.

In order to evaluate ECC on WISPs, we make use of the WISP4.1DL UHF tag developed by Intel Research Seattle. The WISP consists of a tiny low-resource microcontroller (the MSP430F2132) that is attached to a dipole antenna. Next to the microcontroller, the tag features several sensors such as temperature, light, and 3D accelerometer which allows a broad range of RFID and sensor-node applications. There already exist many publications that use the WISP as a demonstrator platform, e.g.,

(Yeager, Sample, & Smith, 2008), (Saxena & Voris, 2009), (Yeager, Holleman, Prasad, Smith, & Otis, 2009), (Smith, Fishkin, Jiang, Mamishev, Philipose, Rea, Roy, Sundara-Rajan, 2005). Only a few publications presented implementations of cryptographic algorithms on the WISP. (Chae, Yeager, Smith, & Fu, 2007), for example, implemented the block cipher RC5 and demonstrated the feasibility of symmetric cryptography on that platform.

In this chapter, we evaluate the feasibility of asymmetric cryptography on WISPs by implementing ECC. We make use of the Montgomery ladder scalar multiplication over the smallest recommended NIST elliptic curve over prime fields, i.e., P-192. Furthermore, we implemented ECC over binary fields using a comparable elliptic curve standardized by ANSI X9.62 using 191 bits. In order to meet the low-resource constraints of WISPs, we applied several optimization techniques. First, we applied different field-multiplication methods that reduce the memory and computational requirements to a minimum. Second, we make use of state of the art ECC formulae to provide efficient computation on the algorithmic level. As a result, we show that a scalar multiplication can be performed in 8.3 seconds at 6.7 MHz on the WISP4.1DL device (featuring no hardware multiplier) and only 1.6 seconds on the WISP when a hardware multiplier is supported. Our binary-field based implementation needs about 2 seconds without needing a hardware multiplier. ECC over prime fields is therefore recommended on WISPs which feature multiplication support, ECC over binary fields is recommended otherwise.

After the introduction, we will give a short overview on ECC. We will describe the basic principles of the public-key technique and explain the different parameters of ECC. Afterwards, we will present the WISP platform we used for demonstration. First, the hardware is described in

Related Content