

Processor core for Elliptic Curve Cryptography

Overview

Secure data encryption is an essential part of modern communication technologies. It can help to prevent unauthorized access to sensitive data. This is particularly important for wireless networks where anyone can eavesdrop on the communication.

In general, symmetric encryption algorithms are used to obtain high data rates. These algorithms use identical keys to encrypt and decrypt data. One big issue with using symmetric algorithms is the key exchange problem. Both communication parties must exchange the key and ensure that the key remains secret. It is usually inconvenient and expensive to find a secure channel for the key exchange.

These problems are solved by asymmetric encryption algorithms. They replace the single shared secret key with a pair of mathematically related keys: one Public Key that can be made publicly available and one secret Private Key. All asymmetric algorithms have in common that they rely on the special properties of one-way functions. In general it is simple to calculate a one-way function, but without additional information it's nearly impossible to calculate the inverse function.

Traditional asymmetric algorithms utilize the multiplication of huge prime numbers as one-way function. Another method, published 1985 by Miller and Koblitz, suggests the use of special operations with elliptic curves as one-way functions. These methods are called Elliptic Curve Cryptography (ECC).

Figure 1 shows the plot of an elliptic curve.

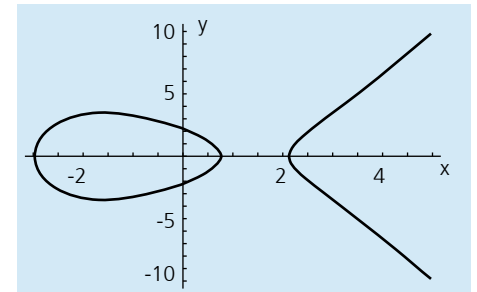


Fig. 1: Elliptic Curve

Advantages of Elliptic Curve Cryptography

More and more communication processes are performed by small and mobile devices which are typically limited in their CPU, memory, battery and bandwidth resources. Special integrated circuits can help to disburden the general purpose CPU from exhausting cryptographic calculations. Often, traditional public-key algorithms can not offer satisfying solutions for this class of mobile devices. At this point, elliptic curve based algorithms are an attractive alternative to traditional methods.

Symmetric Algorithms	Asymmetric Algorithms		Secure Until
	RSA, DH	ECC	
56	417	85	1982
63	622	106	1990
70	952	132	2000
78	1369	146	2010
86	1881	188	2020
93	2493	176	2030
101	3214	191	2040
109	4047	272	2050

Tab. 1: Security comparison for different algorithms [Lenstra: "Selecting Cryptographic Key Sizes", 1999]

Fraunhofer-Institut Photonische Mikrosysteme

Maria-Reiche-Str. 2
01109 Dresden
Phone: +49 (0) 3 51/88 23-0
Fax: +49 (0) 3 51/88 23-266
www.ipms.fraunhofer.de

Contact:
Ines Schedwill
Phone: +49 (0) 3 51/88 23-238
ines.schedwill@ipms.fraunhofer.de

Technical questions:
Dr. Andreas Heinig
Phone: +49 (0) 3 51/88 23-288
andreas.heinig@ipms.fraunhofer.de



Quality Management

We are certified

Voluntary participation in regular monitoring according to ISO 9001:2008

Fraunhofer IPMS reserves the right to change products and specifications without prior notice. This information does not convey any license by any implication or otherwise under patents or other right. Application circuits shown, if any, are typical examples illustrating the operation of devices. Fraunhofer IPMS cannot assume responsibility for any problems rising out of the use of these circuits.

In the case of elliptic curve cryptography the underlying mathematical problem is much more difficult to solve than for traditional algorithms. Due to this fact shorter keys can be used to obtain the same level of security. Generally speaking, a shorter key means less operations and therefore less memory and energy consumption.

Table 1 shows in each line the key length, specified in bit, which is necessary to obtain equivalent security for different algorithms. Currently ECC provides the highest security per bit of any known public-key scheme.

System Concept

Figure 3 shows the fundamental system structure. It consists of two parts: the static core system and the variable protocol part.

The core system executes all basic calculations of the elliptic curve cryptography algorithms. For each partial calculation one high specialized dedicated structural component exists. These components communicate with each other over the optimized system-on-chip bus.

The variable protocol part implements the concrete cryptographic protocol. The present system demonstrates the Diffie-Hellman key exchange. The implementation of other cryptographic protocols based on elliptic curves like the Nyberg-Rueppel signature or the Menezes-Qu-Vanstone key exchange is straightforward. This is based on the fact that all ECC related functions exist in the static core system.

System Configuration

The elliptic curve processor core is written in a hardware description language (VHDL). One of the biggest advantages of this design is the possibility to adjust the configuration in a wide range. The processor macro cell can be used on FPGAs or integrated on ASICs.

The selection of a key length in the range from 30 bit to 458 bit is possible for a concrete implementation. This enables the customer to individually adjust the integrated circuit to the given security requirements.

The application of elliptic curves in cryptographic algorithms requires special multiplication operations. The individual implementation and number

of multiplication cores has a significant influence on the system performance. Therefore, this design offers the possibility to choose the number of multiplication cores in the configuration process. This approach allows the designer to find an ideal compromise between execution time and necessary chip area (figure 2).

Characteristics

- IEEE-Standard 1076-1993 compliant synthesizable VHDL model for utilization as macro cell in ASIC and FPGA designs
- Diffie-Hellman key exchange protocol exists
- Implementation of other protocols based on elliptic curves is straightforward
- Key length can be chosen individually in the range from 30 to 453 bit
- Selectable number of multiplication cores

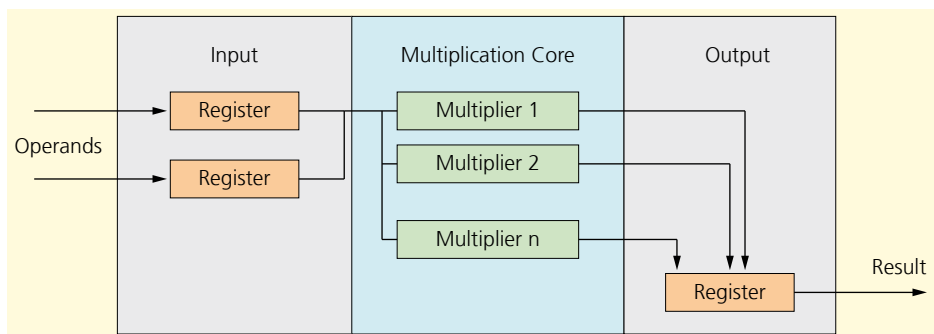


Fig. 2: Multiplication Core

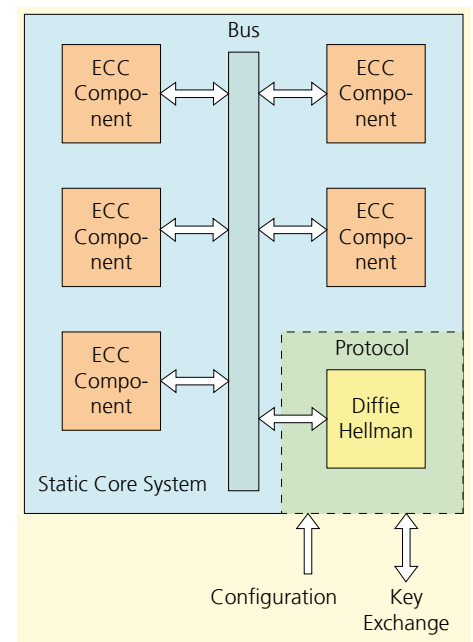


Fig. 3: System Concept