사물인터넷 기기를 위한 경량 Elliptic Curve Diffie-Hellman 키 생성기 하드웨어 설계

Guard Kanda · 류광기
한밭대학교 정보통신전문대학원

Lightweight Hardware Design of Elliptic Curve Diffie-Hellman Key Generator for IoT Devices

Guard Kanda · Kwangki Ryoo
Graduate School of Information and Communication, Hanbat National University
E-mail : guardkanda@gmail.com, kkryoo@hanbat.ac.kr

요 약

새로운 암호화 알고리즘인 ECC (Elliptic Curve Cyptography)는 elliptic curves을 기반으로 하며, 포인트 연산과 Elliptic Curve Discrete Logarithm Problem (ECDLP)을 포함한다. ECDLP는 쉬운 키 생성과 단방향 암호화, 키의 역생성이 불가능한 특징을 가지고 있다. 이러한 ECDLP의 특징은 개인 정보 보호에 매우 강하다. 본 논문에서 제안하는 경량 ECDH 키 생성기 하드웨어는 Elliptic Curve Integrated Encryption Scheme (ECIES) 및 키 공유에 사용할 수 있는 163 비트 공유키를 생성한다. 제안하는 하드웨어 구조에서는 작은 고속 곱셈 알고리즘을 사용하여 확장된 유클리드 알고리즘을 구현했다. 제안하는 하드웨어 구조는 Verilog HDL을 사용하여 설계되었으며, vivado ISE 2016.3과 virtex-7 FPGA 보드를 통해 구현하였다.

ABSTRACT

Elliptic curve cyptography is relatively a current cryptography based on point arithmetic on elliptic curves and the Elliptic Curve Discrete Logarithm Problem (ECDLP). This discrete logarithm problems enables perfect forward secrecy which helps to easily generate key and almost impossible to revert the generation which is a great feature for privacy and protection. In this paper, we provide a lightweight Elliptic Curve Diffie-Hellman (ECDH) Key exchange generator that creates a 163 bit long shared key that can be used in an Elliptic Curve Integrated Encryption Scheme (ECIES) as well as for key agreement. The algorithm uses a fast multiplication algorithm that is small in size and also implements the extended euclidean algorithm. This proposed architecture was designed using verilog HDL, synthesized with the vivado ISE 2016.3 and was implemented on the virtex-7 FPGA board.

키워드
ECC, ECDH, lightweight encryption, ECIES

Ⅰ. INTRODUCTION

An elliptic curve is a two-dimensional (planar) curve defined by an equation involving a cubic power of coordinate x and a square power of coordinate y. A group of these curves, i.e. elliptic cure over a Galois or Finite field. These groups of curves possesses special qualities that naturally makes them suitable to be used in modulus groups of the discrete logarithm problems. Public-key cryptography, developed by Whitfield Diffie and Martin Hellman revolutionized the cryptographic field in the year 1976[1]. Cryptographers Victor Miller[2] and Neal Koblitz[3] independently proposed a cryptosystem whose security relies on the Elliptic Curve DLP (ECDLP). Just like its counterpart IFP, ECDLP is yet another difficult yet simple to state problem that says, given any two points P and Q on an elliptic curve, find an integer n such that P = nQ. Typical example of elliptic curve is shown in figure 1.

From [3], ECDLP is the hardest amongst the mathematical problems for cryptosystem. Consequently, the most important benefit of the ECC is its key size. This shorter key length implies faster processing time as well as lower demand on transmission bandwidth.

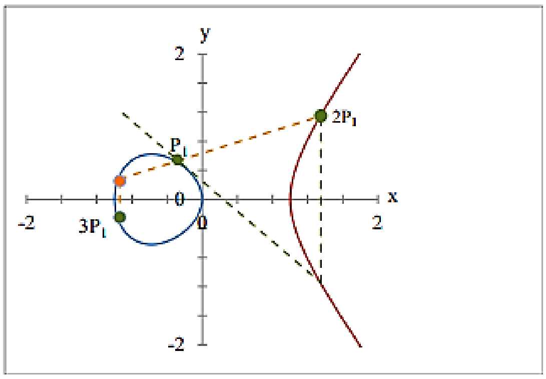


Fig. 1. Elliptic Curve point multiplication

With these IoT devices being limited in terms of resource and ECC having an advantage of using less keys, they become suitable candidates for developing cryptosystem for these devices.

The primary focus of this paper is to design lightweight key sharing algorithm for resource to be used by resource constraint devices based on the Diffie-Hellman shared key exchange algorithm.

II. PROPOSED HARDWARE DESIGN

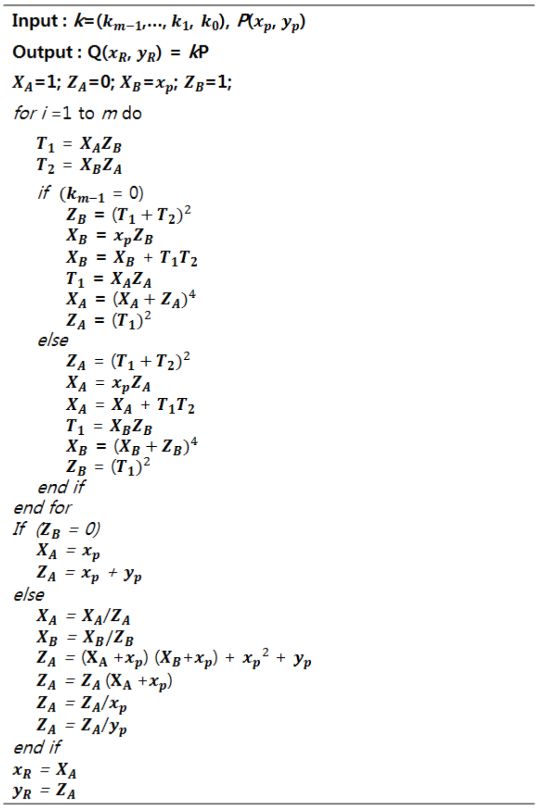
The proposed design was based on the implementation of algorithm 1. The montgomery ladder algorithm for the is the most popular algorithm. The most important fact is that, it can be used both with the affine coordinate and the projective coordinate. For a given associative operation "+" on some elliptic curve E and an m-bit scalar k, the resulting product kP is given by (1)

$$0P=0,\ 1P=P,\ 2P=P+P,\ 3P=P+P+P.... \tag{1}$$

To do this, point R(x,y) must be expressed using projective coordinates. Assuming standard projective coordinates used xA and xB can be expressed as follows (2)

$$\begin{aligned} &Z_{A+B} = (X_A Z_A + X_B Z_B)^2 \\ &X_{A+B} = xpZ_{A+B} + X_A X_B Z_A Z_B \\ &Z_{A+A} = X_A{}^2 Z_A{}^2\ ,\ X_{A+A} = X_A{}^4 + bZ_A{}^4 \end{aligned} \tag{2}$$

Algorithm 1 from figure 2 computes R = kP with possible sequencing of the operations.



```
Input : $k$=($k_{m-1}$,..., $k_1$, $k_0$), $P(x_p, y_p)$
Output : Q($x_R$, $y_R$) = $kP$
$X_A$=1; $Z_A$=0; $X_B$=$x_p$; $Z_B$=1;
for $i$ =1 to $m$ do
    $T_1 = X_A Z_B$
    $T_2 = X_B Z_A$
    if ($k_{m-1}$ = 0)
        $Z_B = (T_1 + T_2)^2$
        $X_B = x_p Z_B$
        $X_B = X_B + T_1 T_2$
        $T_1 = X_A Z_A$
        $X_A = (X_A + Z_A)^4$
        $Z_A = (T_1)^2$
    else
        $Z_A = (T_1 + T_2)^2$
        $X_A = x_p Z_A$
        $X_A = X_A + T_1 T_2$
        $T_1 = X_B Z_B$
        $X_B = (X_B + Z_B)^4$
        $Z_B = (T_1)^2$
    end if
end for
If ($Z_B$ = 0)
    $X_A = x_p$
    $Z_A = x_p + y_p$
else
    $X_A = X_A / Z_A$
    $X_B = X_B / Z_B$
    $Z_A = (X_A + x_p)(X_B + x_p) + x_p{}^2 + y_p$
    $Z_A = Z_A (X_A + x_p)$
    $Z_A = Z_A / x_p$
    $Z_A = Z_A / y_p$
end if
$x_R = X_A$
$y_R = Z_A$
```

Fig. 2. Montgomery Ladder based Point Multiplier Algorithm

For the complete execution of algorithm in figure 2, basic computing modules were designed in mod f(z). As can be inferred from algorithm in figure 2, these modules are multipliers, dividers, squaring. The squaring module implemented is based on the approach presented in[4]. That is simply inserting zeros after each bit in the original. Addition in mod

2 is also implemented by a simple XOR of the two m-bit operands. The addition and squaring are executed in a single cycle. The multiplier executes in *m*-cycles and the divider in 2*m*-cycles.

III. EXPERIMENTAL RESULTS

In this section, we analyze the result of our design and compare other ECC point multiplication hardware implementations. The design was implemented using vivado ISE design suit 2016.3 and verilog HDL.

Table 1 Comparison of different ECC point multiplier for 163 bit

	Area		**Freq**
	LUTs	**FFs**	**(KHz)**
[5]	14203	26557	263
[6]	3806	4807	550
[7]	9670	-	221
proposed	3637	2679	325

The design implemented on a virtex 7 device required 3637 LUTs. From table 1, it is seen that, a 169 reduction in LUTs as compared to the design of [9] which shows a 5% decrease in the number of LUTs and about 45% decrease in the number of FFs. Consequently, the operating frequency for this paper was reduced to a maximum of 325 MHz as compared to that of [9].

Ⅳ. CONCLUSION

In this paper, we present a hardware implementation of the most time consuming ECC point multiplication. The result obtained shows that the proposed design reduces the area of the current design at the expense of operating frequency to enable its use in resource constrained devices for IoT. For Future work, we hope to further improve upon the operating frequency and also to implement a complete Elliptic Curve Integrated Encryption Scheme (ECIES) based on the point multiplier which is the main computation for ECDH.

Acknowledgments

This research was supported by the MSI(Ministry of Science, ICT and Future Planning), Korea, under the Global IT Talent support program(IITP-2017-0-01681) and Human Resource Development Project for Brain scouting program(IITP-2016-0-00352) supervised by the IITP(Institute for Information and Communication Technology Promotion)

REFERENCE

[1] W. Diffie and M. E. Hellman, “New directions in cryptography,” IEEE Transactions in Information Theory, Vol. 22, No. 6, pp. 644-654, Nov. 1976.

[2] V. S. Miller, “Use of elliptic curves in cryptography,” Lecture Notes in Computer Science, Vol. 218, pp. 417-426, May, 1986.

[3] N. Koblitz, "Elliptic curve cryptosystems", Mathematics of Computation, Vol 48, pp. 203-209, January, 1987.

[4] F. Rodríguez-Henríquez, N. A. Saqib, and A. Díaz-Pérez, “A fast parallel implementation of elliptic curve point multiplication over GF(2m),” Micro- process. Microsyst., Vol. 28, No. 5-6, pp. 329-339, Aug. 2004.

[5] H. Mahdizadeh and M. Masoumi, “Novel Architecture for Efficient FPGA Implementation of Elliptic Curve Cryptographic Processor Over GF(2163),” IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 21, No. 12, pp. 2330-2333, Dec. 2013.

[6] T. T. Nguyen and H. Lee, “Efficient Algorithm and Architecture for Elliptic Curve Cryptographic Processor,” Journal of Semiconductor and Science, Vol. 16, No. 1, pp.118-125, Feb. 2016.

[7] A. Sghaier, M. Zeighid, C. Massoud, and M. Machout, “Design and Implementation of Low Area/Power Elliptic Curve Digital Signature Hardware Core,” Electronics Journal-MDPI, Vol. 2, No. 46, pp. 1-23, Jun. 2017.