Memorias del XVI Congreso Latinoamericano
de Control Automático, CLCA 2014
Octubre 14-17, 2014. Cancún, Quintana Roo, México

IMPLEMENTACION DE UNA CURVA ELIPTICA APLICADA A UNA WSN LIMITADA EN HARDWARE

I.Chinchay.[*], H.Kaschel.[**], R.Abarzua[***]

[*]*Departamento de Electrónica y Automática, Facultad de Ingeniería,Universidad de Piura, Urb. San Eduardo s/n, Piura, Perú (e-mail: italo.chinchay@udep.pe)*
[**]*Universidad de Santiago de Chile, Avenida Libertador Bernardo O'Higgins # 3363(e-mail: hector.kaschel@usach.cl)*
[***]*Universidad de Santiago de Chile, Avenida Libertador Bernardo O'Higgins # 3363 (e-mail: rodrigo.abarzua@usach.cl)*

Resumen: Las Redes de Sensores Inalámbricas (Wireless Sensor Network: WSN), utilizan dispositivos llamados nodos, formados por un hardware y un software con capacidades limitadas, porque su característica principal es el bajo costo, dimensiones pequeñas y de bajo consumo energético. Con este principio, es complicado establecer un esquema de seguridad robusto que asegure un nivel aceptable de seguridad a una aplicación que lo requiera. Por esto se hace necesario implementar un esquema de seguridad que sea ligero y a la vez seguro. Uno de los que la literatura recomienda es el uso de la criptografía en curva elíptica (ECC=Elliptic Curve Cryptography), como base para implementar diferentes esquemas de seguridad, como por ejemplo el ECDSA(Elliptic Curve Digital Signature Algorithm), el ECDH(Elliptic Curve Diffie-Hellman) y el ECDLP(Elliptic Curve Discrete Logarithm Problem). Este trabajo proporciona una explicación clara de la ECC y su implementación en un nodo WSN.

Palabras claves : sensor, Wireless, *security analysis, cipher*, ECC

I. INTRODUCCIÓN

Las Redes de Sensores Inalámbricos (WSN: Wireless Sensor Network) (IEEE Standard, 2011)por su concepción original, no poseen un hardware robusto que permita implementar un sistema de seguridad sofisticado, como por ejemplo AES (Advanced Encryption Standard) (Darrel *et al.,* 2004)o RSA (Rivest-Shamir-Adleman) (Darrel *et al.*, 2004), con longitudes de clave mayores a 192 bits, porque esto implica un costo de cómputo alto con mayores recursos de memoria de trabajo y de almacenamiento de programa.

Ante esta situación, se recomienda un esquema de encriptamiento ligero de clave pública (asimétrico) y rápido; uno de los recomendados en la literatura, en situación de restricciones de hardware, es el uso de la curva elíptica, que logran aceptable nivel de seguridad con longitudes de llave más pequeñas.

La curva elíptica, tiene un modelo de trabajo jerárquico, mostrado en la figura 1.

Se compone de un grupo de operaciones, sobre un campo finito de números; las cuales se combinan para encontrar un resultado o ser parte de un algoritmo. A esto se le llama "jerarquía de operaciones" (Praful *et al.*, 2013).

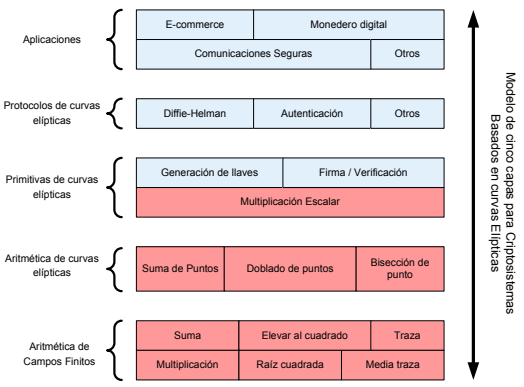

Figura 1. Jerarquía de operaciones en ECC

Las operaciones básicas (Darrel *et al.*, 2004), (Praful *et al.*, 2013) y (Purohit*et al.*, 2010) en la curva elíptica son: el doblado de un punto y la suma de dos puntos de la curva. Pero estas a su vez deben utilizar otras operaciones aritméticas tales como: resta, inversa, el cuadrado, la multiplicación entre otras y por utilizar números grandes, se hace necesario utilizar la operación en modulo, "$modp$" o también llamada "reducción".

La ecuación característica de una curva elíptica sigue la forma estándar (FIPS PUB 186-4, 2013):

$$E: y^2 \equiv x^3 + ax + b\ modp \qquad (1)$$

Y se trabaja en el plano cartesiano(x, y).

El punto resultado de la operación en la curva elíptica, se encuentra con una multiplicación escalar:

$$R = k * P \qquad (2)$$

Por ejemplo en la figura 2, se desarrolla la multiplicación escalar.

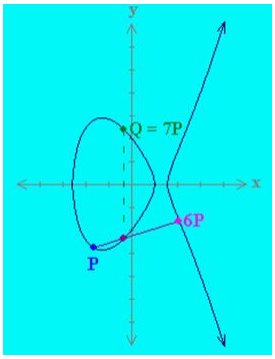

Figura 2. Ejemplo gráfico

$y^2 = x^3 + 5x + 4$
$P = (-1.65, -2.79)$

$Q = 7 * P$
Q= $(-0.35, -2.39)$

Las operaciones necesarias, ahora deben ser resueltas en el nodo WSN, el cual tiene recursos limitados.

La organización de este *paper* es como sigue: en la sección II se describen las operaciones aplicadas en una curva elíptica bajo el estándar NIST(FIPS PUB 186-4, 2013); en la sección III se describe la implementación del algoritmo de la curva elíptica en el nodo WSN. Finalmente, en la sección IV, se entregan las conclusiones principales y las futuras líneas de desarrollo asociadas.

II. OPERACIONES APLICADAS EN UNA CURVAELIPTICA BAJO EL ESTANDAR NIST

Las operaciones matemáticas en curva elíptica son: el doblado de un punto y la suma de dos puntos en modulo "p", donde "p" es un número primo muy grande y las operaciones son reducidas en modulo "p" "mod p ". Estas operaciones se reflejan al ejecutar la multiplicación escalar, entre un número entero y un punto de la curva R = k ∗ P. Por ejemplo, al descomponer en sumandos la operación siguiente :

$$R = 7 * P = (P + (P + (P + \big(P + (P + 2P)\big))))$$

Aunque no es la única forma de descomponer, se puede observar el doblado y la suma de un punto:

El doblado de un punto: $2P$

Y la suma de dos puntos: $P + 2P$

Estas operaciones pueden ser resueltas con solo los datos (x, y) del punto "P". La solución en forma gráfica, se puede observar en las figuras 3 y 4.

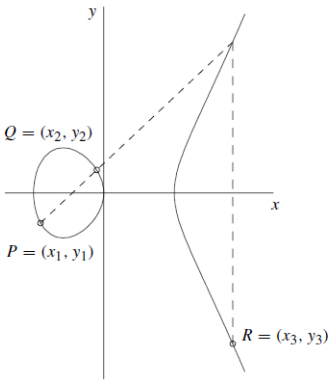

Figura 3. Suma de dos puntos de curva (Darrel *et al.*, 2004)

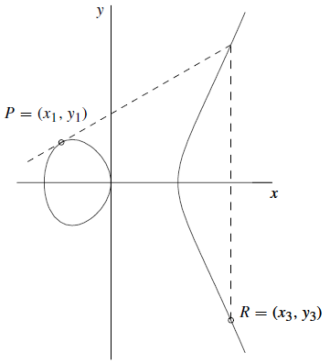

Figura 4. Doblado de un punto de curva (Darrel *et al.*, 2004)

De forma analítica (Darrel *et al.*, 2004), el cálculo del punto resultado $R(x_3, y_3)$ sigue la siguiente ecuación.

$$P(x_1, y_1) + Q(x_2, y_2) = R(x_3, y_3)$$

$$x_3 = \lambda^2 - x_1 - x_2 modp$$
$$y_3 = \lambda(x_1 - x_3) - y_1 modp$$

$$\lambda \begin{cases} Doblado: \ P = Q \rightarrow \lambda = \dfrac{3x_1^2 - 3}{2y_1} modp \\ suma: \quad P \neq Q \rightarrow \lambda = \dfrac{y_2 - y_1}{x_2 - x_1} modp \end{cases}$$

El valor de "λ" cambia según si la operación es un doblado o una suma del punto de curva elíptica.

Ahora, pasando al campo real del cálculo, los valores utilizados se toman del estándar NIST, para una curva Elíptica:

Ecuación recomendada (FIPS PUB 186-4, 2013):

$$E: y^2 \equiv x^3 - 3x + b$$

Los parámetros de la curva recomendados por estándar NIST, y utilizados en la implementación son:

Orden de los datos, {[LSB] ...[MSB]}

Primo p: = { FF,FF,FF,FF,FF,FF,FF,FF,FE,FF,FF,FF, FF,FF,FF,FF,FF,FF,FF,FF,FF,FF,FF,FF }

Orden n= {31,28,D2,B4,B1,C9,6B,14,36,F8,DE,99, FF,FF,FF,FF,FF,FF,FF,FF,FF,FF,FF,FF }

Coefi. b= { B1,B9,46,C1,EC,DE,B8,FE,49,30,24,72, AB,E9,A7,F,E7,80,9C,E5,19,5,21,64 }
Punto G:
x[ ] = { 12,10,FF,82,FD,A,FF,F4,0,88,A1,43, EB,20,BF,7C,F6,90,30,B0,E,A8,8D,18 }
y[ ] = { 11,48,79,1E,A1,77,F9,73,D5,CD,24,6B, ED,11,10,63,78,DA,C8,FF,95,2B,19,7 }

Con estos valores se puede hacer un ejemplo de cálculo en el módulo WSN de:

$R(x_3, y_3) = k * \mathrm{G}(x, y)$.

k[]={ 18,ED,62,DA,51,3B,8E,BC,44,93,88,B0, 9A,D1,9A,71,72,B1,60,CC,FD,84,8E,E0,}

$R(x_3)$[]={ 51,6F,D9,D6,13,6B,B1,AD,51,AD,0,34, E7,7E,5F,89,80,7B,BE,97,56,96,8D,30,}
$R(y_3)$[]={ 94,B9,6,CF,6C,F1,86,70,49,A6,4E,EB, E1,F0,FB,B0,D,7,BD,C5,33,C1,67,5F,}

El valor de "k" ahora está representado por un punto de la curva elíptica. Esta operación básica es parte de varios algoritmos de seguridad que permiten realizar: encriptamiento, autenticación e intercambio de claves seguras y para este acaso particular con una longitud de clave de 24 byte (192 bits).

III. IMPLEMENTACION DEL ALGORITMO DE UNA CURVA ELIPTICA EN EL NODO WSN

El algoritmo ECC se implementa sobre un nodo WSN formado por un módulo Arduino y un módulo Xbee, según muestra la figura 5. Las funciones de cada módulo son:

El módulo Arduino(Arduino**)**, ejecuta las operaciones de ECC, obtenidas de la librería GitHuby que después se pueden combinar para formar un algoritmo de seguridad, como por ejemplo ECDSA, ECDH y ECDLP (Darrel et al., 2004), (Paaret al., 2010).

El módulo Xbee (Xbee), (ZigBee), transportará la información, en forma de un punto de la curva elíptica, como un dato dentro de su trama. La trama tiene una estructura adecuada para poder identificar las partes del dato.

Lo anterior, se logra utilizando la trama tipo API, que maneja el Xbee. El estándar IEEE 802.15.4 define una trama API, según la se muestra en la figura 6.

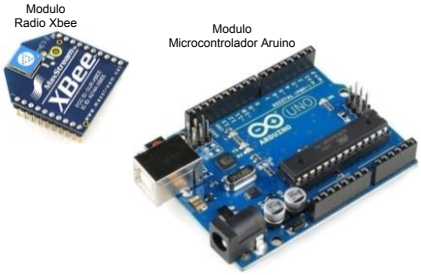

Figura 5. Nodo WSN

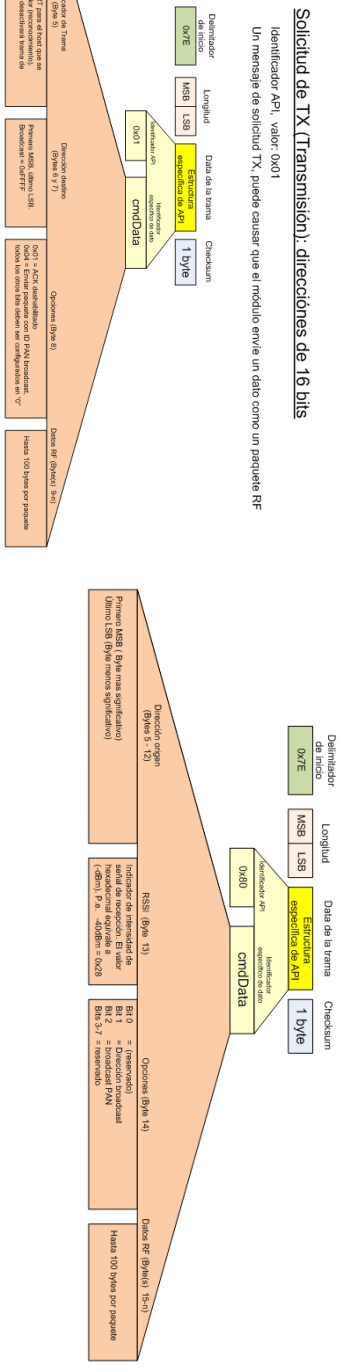

Figura 6. Trama API de transmisión y recepción (MaxStream)

El formato de trama diseñado para transportar el dato de un punto de curva elíptica tiene 58 bytes y se muestra en la figura 7.

Trama de transmisión

0x7E	0x00	0x36	0x01	0x00	$DH	$DL	0x01	Dato (48 bytes)	Ctrol	FCS

Trama de recepción

0x7E	0x00	0x36	0x81	$SH	$SL	RSSI	0x00	Dato (48 bytes)	Ctrol	FCS

Figura 7. Formato de trama API de 58 bytes.

En el caso más elemental de transmisión, un nodo WSN debe hacer la toma de información, luego encriptarla con ECDLP y finalmente transmitirla de forma inalámbrica siguiendo el estándar WSN IEEE 802.15.4. Esto se resume en la figura 8.

Este mecanismo asegura que la información transmitida tendrá la confidencialidad necesaria, en el medio en que es transmitida.

En la tabla 1, se aprecia que con el mismo nivel de seguridad, la curva elíptica logra tener menor carga de transmisión que el RSA (384bits < 7680bits).AES es también una opción, pero es un algoritmo de clave simétrica, el cual no es recomendado por el NIST.

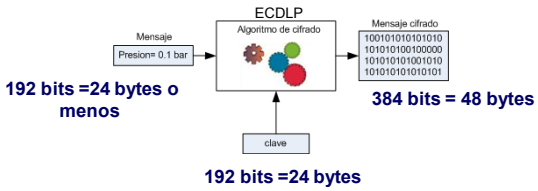

Figura 8. Proceso de encriptamiento en nodo WSN

Tabla 1. Recomendación NIST – 2012

Date	Minimum of Strength	Symmetric Algorithms	Asymmetric	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash (A)	Hash (B)
2010 (Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1** SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
2011 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
> 2030	128	AES-128	3072	256	3072	256	SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
>> 2030	192	AES-192	7680	384	7680	384	SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512
>>> 2030	256	AES-256	15360	512	15360	512	SHA-512	SHA-256 SHA-384 SHA-512

Un algoritmo completo se muestra en la figura 9. Donde primero se hace la autenticación (ECDSA), luego un intercambio de clave pública (ECDH) y finalmente el ECDLP.

En todos los procesos se hace necesario realizar operaciones en curva elíptica, por lo que la implementación de las librerías ECC en el nodo, es prioritario. La figura 10, muestra el resultado del cálculo ECC a un dato de 24 byte, realizado por el módulo Arduino, indicando los tiempos de encriptamiento y desencriptamiento.

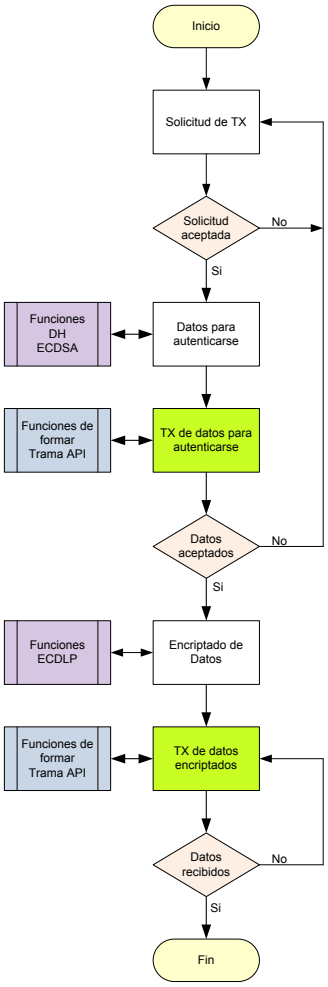

Figura 9. Operaciones de un algoritmo de seguridad: Autentica y encripta información.

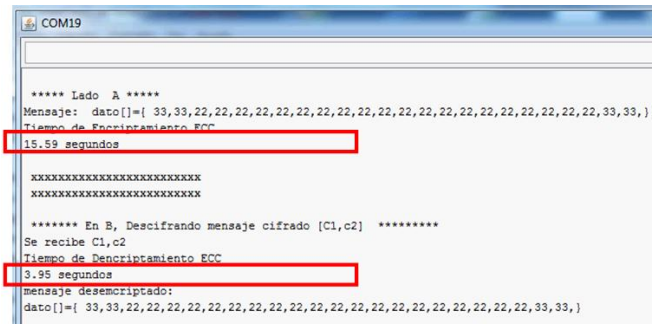

Figura 10. Resultado del cálculo ECC realizado a un dato de 24 bytes.

IV. CONCLUSIONES

La criptografía con ECC reduce los tiempos de ejecución, ahorra consumo de energía y logra un nivel de seguridad aceptable. Esto lo hace atractivo para las aplicaciones móviles y con bajos recursos de hardware. Su uso puede ser

extendido en las tarjetas inteligentes, nodos WSN y aplicaciones RFID, que utilizan menos memoria y potencia.

La implementación de la librería ECC en un módulo Arduino, abre las posibilidades de probar diferentes situaciones (Jaydip*et al.*, 2009), aprovechando la flexibilidad de programación del Arduino y con la flexibilidad de la trama API del módulo Xbee, para modificar su estructura de dato, se convierte en un sistema para pruebas de laboratorio, diferente a ser utilizado en una aplicación específica.

AGRADECIMIENTOS

Esta investigación se realizó con los aportes financieros del proyecto DICYT USACH Código 061213KC “Diseño e implementación de una Red IWSN (Industrial Wireless Sensor Network), tolerante a fallas, eficiente y con alta seguridad” de la Universidad de Santiago de Chile y del Laboratorio de Control y Automática de la Universidad de Piura, "Fondo para la Innovación, Ciencia y Tecnología (FINCyT)", Perú, bajo el proyecto 145-FINCyT-IA-2013.

REFERENCIAS

Arduino [Online]. http://arduino.cc/es/

BlueKrypt Your Securty Expert. BlueKrypt Your Securty Expert. [Online]. ttp://www.keylength.com/en/4/.

York: Springer, 2010.

Darrel Hankerson, Alfred Menezes, and Scott Vanstone, Guide to Curve Elliptic, primera ed.: Springer, 2004.

FIPS PUB 186-4, "Digital Signature Standard (DSS), Federal Information Processing Standards Publication," National Institute of Standards and Technology, july 2013.

GitHub - Contribuciones de Ken MacKay. [Online].https://github.com/kmackay/micro-ecc

IEEE Standard for Local and metropolitan area networks, "Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)," LAN/MAN Standards Committee IEEE Computer Society, 2011.

Paar Christof and Pelzl, Understanding Cryptograpphy. New

Purohit G.N., Asmita Singh Rawat. "Efficient Implementation of Arithmetic Operations in ECC over Binary Fields", 2010 International Journal of Computer Applications, pp.0975 – 8887, Volume 6– No.2, September 2010.

Praful Kumar Singh, Mrityunjay Kumar Choudhary. "Scalar Multiplication Algorithms of Elliptic Curve Cryptography over GF (2m)", 2013 International Journal of Innovative Technology and Exploring Engineering (IJITEE), pp. 2278-3075, Volume-3, Issue-1, June 2013.