Criptografia Leve para Dispositivos IoT

Iago Galvão * **Samaherni Dias** * **Kurios Queiroz** *

* *Laboratório de Automação, Controle e Instrumentação (LACI), UFRN, Natal, RN, Brasil, (https://laci.ufrn.br)*

Abstract: Smart environments are part of the rapid development of digital transformation, and the growing need for multiple connections with different devices is driving research attention toward the Internet of Things (IoT) as a way of communicating with objects. Data transmitted widely and openly, whether in industries, homes, buildings or cities, is vulnerable to attacks that capture private information or even control devices without proper protection measures. Therefore, secure communication is mandatory to ensure an efficient and reliable system, as well as the application methods, must be updated to anticipate the advance of attacks. Thus, the Rivest-Shamir-Adleman (RSA) asymmetric encryption method, which is widely, is taken as a basis to compare the application in IoT systems of a lightweight cipher (algorithm), using Elliptic Curve Cryptography (ECC) which requires smaller key sizes to match the security level of RSA.

Resumo: Ambientes inteligentes fazem parte do rápido desenvolvimento da transformação digital, e a crescente necessidade de múltiplas conexões com diferentes dispositivos está direcionando a atenção da pesquisa para a Internet das Coisas (IoT) como forma de comunicação com objetos. Os dados transmitidos de forma ampla e aberta, seja em indústrias, residências, prédios ou cidades, é um ponto vulnerável para ataques que capturam informações privadas ou mesmo controlam dispositivos sem as devidas medidas de proteção. Portanto, a comunicação segura é obrigatória para garantir um sistema eficiente e confiável, bem como, os métodos de aplicação devem estar atualizados para antecipar o avanço dos ataques. Assim, o método de criptografia assimétrico Rivest-Shamir-Adleman (RSA), que é amplamente utilizado, é tomado como base para a comparação. Sistemas IoT devido as suas restrições requerem criptografia de cifra (algoritmo) leve, como por exemplo a Criptografia de Curva Elíptica (ECC) que necessita de menores tamanhos de chaves para equiparar-se ao nível de segurança do RSA.

Keywords: lightweight encryption; ECC; IoT security; low power/voltage; RSA.
Palavras-chaves: criptografia leve; ECC; segurança Iot; baixa potência/tensão; RSA.

1. INTRODUÇÃO

A transformação digital após a quarta revolução industrial resulta em conectividade no geral, tanto interações computador-computador como humano-computador necessitam de dispositivos confiáveis para trocas de informações seguras. Estima-se que até 2030 serão mais de 29 bilhões de conexões em todo o mundo de dispositivos IoT - *Internet of Things* (Statista, 2022) que, para um ecossistema seguro, toda sua arquitetura deve possuir o nível de segurança adequado. Dentre as camadas da arquitetura IoT (física/percepção, *network* e aplicação), a comunicação é a camada mais susceptível a ataques, principalmente na troca de informações transmitida amplamente (Bhardwaj et al., 2017).

A criptografia é uma técnica de segurança ativa, reconhecida pela eficiência em assegurar a troca de dados e categoriza-se em simétrica e assimétrica. Este trabalho se concentra em criptografia assimétrica.

Também conhecido como criptografia de chave pública, a criptografia assimétrica é qualquer sistemas de criptografia que utiliza um par de chaves, sendo uma pública e outra privada. A chave pública pode ser amplamente disseminada e é utilizada para encriptar a mensagem, enquanto a chave privada deve ser mantida reservada e é utilizada para decifrar a mensagem criptografada (ver Figura 1). O propósito de uma criptografia assimétrica é transmitir uma mensagem de forma segura em um canal inseguro. O que significa que a menagem enviada apenas poderá ser decifrada pela pessoa correta. A criptografia assimétrica se baseia na existência de uma função arapuca, ou seja, um função que é fácil de calcular em uma direção, mas é difícil calcular seu inverso sem uma informação especial, chamada arapuca (Koblitz et al., 2004).

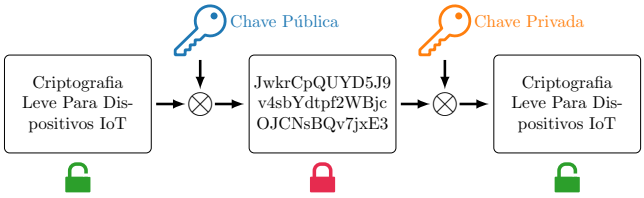

Figura 1. Ilustração do sistema de criptografia assimétrica

Técnicas com duas chaves (pública e privada) possuem uma maior segurança em relação ao uso de uma única chave para cifra dos dados. Normalmente, para o aumento

da segurança, eleva-se também o custo computacional para aplicação de uma codificação assimétrica em relação a simétrica.

Portanto, os maiores desafios para aplicação em dispositivos IoT com limitado processamento, memória e/ou bateria no desenvolvimento de uma cifra assimétrica, é não equiparar-se ao nível de segurança de uma criptografia de única chave. O algorítimo deve ser o mais eficiente possível e as trocas de informações necessitam atingir os seguintes requerimentos: confidencialidade, identificação, autenticação e *nonrepudiation* (Carracedo et al., 2018).

São exemplo de criptografia assimétrica a RSA (Rivest-Shamir-Adleman), a troca de chaves de Diffie-Helman, ECC (*Elliptic-Curve Cryptography*), entre outras. Neste trabalho serão detalhadas a RSA, por ser uma das mais populares, e a ECC por ser a investigada neste trabalho para aplicação em IoT.

A ECC é amplamente utilizada, como a principal concorrente do sistemas de criptografia RSA, pela enorme dificuldade em determinar o logaritmo discreto de um elemento de uma curva elíptica aleatória, apenas com um único ponto. Isto posto, a ECC é capaz de prover o mesmo nível de segurança da RSA, porém utilizando chaves menores, o que influencia diretamente na redução do uso de memória, custo computacional, consumo de energia e o limite de banda (Hassan e Qamar, 2010).

A proposta desse trabalho é comparar duas metodologias de criptografias assimétricas: a mais consolidada a Rivest-Shamir-Adleman - RSA e a *Elliptic Curve Cryptography* - ECC (Criptografia de Curva Elíptica) que proporciona um nível de segurança equivalente, demandando menos *bits* nas suas chaves.

O texto está organizado da seguinte forma: na seção 2 são apresentadas algumas definições preliminares utilizadas; na seção 3 é apresentado o sistema criptográfico RSA; em seguida, na seção 4 o sistema criptográfico ECC é detalhado; os resultados da comparação da aplicação dos sistemas criptográficos RSA e ECC são apresentados na seção 5; e, por fim, as conclusões na seção 6 resumem as tratativas apresentadas e propõe trabalhos futuros.

2. NOTAÇÃO E DEFINIÇÕES PRELIMINARES

Seja o módulo um número inteiro positivo $n \in \mathbb{N}^*$. São considerados congruentes deste módulo dois números inteiros a, b, se existe um inteiro k tal que

$$a - b = k \cdot n, \tag{1}$$

desta forma, pode-se definir a congruência módulo n como

$$a \equiv b \pmod{n}. \tag{2}$$

De acordo com o Pequeno Teorema de Fermat, se p é um número primo, então para qualquer inteiro a, o número $a^p - a$ é um inteiro múltiplo de p. Utilizando uma notação de aritmética modular

$$a^p \equiv a \pmod{p}. \tag{3}$$

Se a não é divisível por p, isto é, se a é coprimo de p, pelo teorema é possível afirmar que $a^{p-1} - 1$ é um número inteiro múltiplo de p, ou seja,

$$a^{p-1} \equiv 1 \pmod{p}. \tag{4}$$

De acordo com a função totiente de Euler $\phi(x)$ é a contagem k de inteiros positivos até x que são coprimos com respeito a x, ou seja,

$$\phi(x) = \{k, x \in \mathbb{N} \mid 0 < k \leq x \wedge \text{mdc}(k, x) = 1\}, \tag{5}$$

em que $\text{mdc}(k, x)$ representa o máximo divisor comum entre k e x.

Um grupo é um conjunto não vazio de elementos com uma operação binária que satisfaz as seguintes propriedades: fecho, associatividade, existência de elemento neutro, e existência de elemento simétrico. Assim, seja G um conjunto e $+$ uma operação binária definida sobre G, tem-se

$$G + G \implies G(x, y) \implies x + y. \tag{6}$$

Um anel R é uma estrutura algébrica que consiste em um grupo associado a duas operações binárias $+$ (adição) e $\cdot$ (multiplicação) que satisfaz as seguintes propriedades: $(R, +)$ é um grupo abeliano, $(R, \cdot)$ é um monoide tal que a multiplicação distribui sobre a adição e

$$R + R \implies R(x, y) \implies x + y \tag{7}$$

$$R \cdot R \implies R(x, y) \implies x \cdot y \tag{8}$$

Um corpo $\mathbb{F}$ é um tipo especial de anel no qual cada elemento não nulo possui um elemento multiplicativo inverso, ou seja,

$$(\forall x \in \mathbb{F} \setminus \{0\})(\exists y \in \mathbb{F}) \ : \ x \cdot y = 1. \tag{9}$$

Um corpo finito $\mathbb{F}_q$, sendo q um número inteiro, é um corpo em que o conjunto dos elementos é finito.

Seja um polinômio mônico de grau n dado por

$$P(x) = \prod_{u=1}^{n} (x - r_u) = \sum_{u=0}^{n} p_u x^u, \quad p_n = 1, \tag{10}$$

com raízes $r_1, r_2, \ldots, r_n$, o discriminante de $P(x)$ será

$$D_x(P) = p_n^{2n-2} \prod_{i<j}^{n} (r_i - r_j)^2 \tag{11}$$

e o coeficiente do segundo termo de maior potência será o valor negativa do somatório das raízes do polinômio, ou seja,

$$p_{n-1} = -\sum_{u=1}^{n} r_u. \tag{12}$$

3. SISTEMA DE CRIPTOGRAFIA RSA

O RSA (Rivest-Shamir-Adleman) é um dos sistemas de criptografia assimétrica mais utilizados, ele consiste em uma chave pública para encriptar e uma chave privada para decifrar, e é considerado seguro devido a dificuldade de fatoração do produto de dois números primos grandes (Mosenia e Jha, 2017).

A função arapuca do RSA é escrita como módulo de exponenciação de um número composto e está relacionada ao problema de fatoração de números primos. Em outras palavras, é muito simples multiplicar números, mas pode ser muito difícil fatorar números.

3.1 Gerando as chaves pública e privada

No RSA, são necessários dois números primos grandes p, q, um expoente e para encriptação e um expoente d para

decifrar a mensagem. Para gerar as chaves deve-se proceder de acordo com os seguintes passos:

(1) Dois números (p e q) grandes, distintos e primos são gerados.

(2) Multiplica-se os números primos entre si,
$$n = p \cdot q. \tag{13}$$

(3) Calcula-se a função tontiente de Euler para n,
$$\phi(n) = (p-1) \cdot (q-1). \tag{14}$$

(4) O expoente da chave pública é obtido ao se escolher um número inteiro e, dentro do intervalo
$$1 < e < \phi(n), \tag{15}$$
que seja coprimo a $\phi(n)$, ou seja,
$$\text{mdc}(e, \phi(n)) = 1. \tag{16}$$

(5) O expoente da chave privada d deve satisfazer a função
$$e \cdot d \equiv 1 \pmod{\phi(n)}. \tag{17}$$

Assim, tem-se as duas chaves: a pública formada pelo par (n, e) e a privada formada por d (Rivest et al., 1978).

3.2 Criptografando e Decifrando Mensagens

Para encriptar uma mensagem m utilizando o sistema de criptografia RSA deve-se, de posse da chave pública (n, e), calcular
$$m^e \equiv c \pmod{n}, \tag{18}$$
em que c é a mensagem m codificada.

Para decifrar a mensagem codificada c utilizando o sistema de criptografia RSA deve-se, de posse da chave privada d, calcular
$$c^d \equiv m \pmod{n}. \tag{19}$$

4. CRIPTOGRAFIA DE CURVA ELÍPTICA

A criptografia de curva elíptica (ECC - *Elliptic-Curve Cryptography*) é uma abordagem de criptografia assimétrica, proposta de forma independente por Miller (1985) e Koblitz (1987), que realiza a criptografia das mensagens baseado em curvas elípticas em campos finitos.

A função arapuca da ECC é baseada na dificuldade do problema do logaritmo discreto em curvas elíptica, ou seja, em calcular o logaritmo discreto de um elemento de uma curva elíptica aleatório em relação a um ponto base conhecido publicamente. Desta forma, a função arapuca da ECC está na facilidade de calcular a multiplicação de um ponto na curva e da incapacidade de calcular o multiplicando dado o ponto original da curva e o ponto resultante do produto (Koblitz, 1987).

O caso geral de uma curva elíptica E sobre um corpo $\mathbb{F}$ pode ser representada por
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{F}, \tag{20}$$
em que $E(\mathbb{F})$ denota o conjunto de pontos $(x, y) \in \mathbb{F}^2$ que satisfazem a essa equação, juntamente com um "ponto no infinito" definido por O. Se $\mathbb{K}$ é uma extensão qualquer do corpo $\mathbb{F}$, então $E(\mathbb{K})$ denota um conjunto de pontos $(x, y) \in \mathbb{K}^2$ que satisfaz (20). Para que a curva em (20) seja uma curva elíptica para criptografia ela tem que ser suave.

Uma curva elíptica definida sobre um corpo $\mathbb{F}$ com característica de Euler-Poincaré diferente de 2 e 3, sem perda de generalidade pode ser caracterizada por
$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}, \quad \text{char } \mathbb{F} \neq 2, 3. \tag{21}$$
Nesse caso, a condição de que a curva seja suave equivale a exigir que a cúbica à direita não tenha raízes múltiplas. Isto ocorre se e somente se o discriminante de
$$x^3 + ax + b \tag{22}$$
for diferente de zero, ou seja,
$$-(4a^3 + 27b^2) \neq 0. \tag{23}$$
Para qualquer extensão $\mathbb{K}$ do corpo $\mathbb{F}$, o conjunto $E(\mathbb{K})$ forma um grupo abeliano cujo o elemento identidade é O.

Uma curva elíptica sobre os números reais é o conjunto de pontos (x, y) que satisfaz uma equação dada por
$$y^2 = x^3 + ax + b, \tag{24}$$
em que x, y, a, b são números reais.

A ideia é que os pontos em uma curva elíptica possua estrutura algébrica, desta forma, permitindo a realização de operações binárias a dois pontos desta curva. Um grupo de curvas elípticas sobre números reais ($\Re$) consiste nos pontos da curva elíptica, juntamente com um ponto especial O, chamado de ponto no infinito, o qual será o elemento identidade na operação de adição. A adição de dois pontos em uma curva elíptica pode ser realizada de duas formas, gráfica e algébrica. Em ambos os casos, o segredo é encontrar o terceiro ponto da interseção entre a curva elíptica e uma reta através dos dois pontos dados nesta curva.

Seja E uma curva elíptica sobre os números reais de acordo com a equação (24) e P e Q dois pontos em E. Defini-se o negativo de P e a adição de $P + Q$ pelas seguinte regras:

(1) Se P é um ponto no infinito O, então $-P$ é O. Para qualquer ponto Q defini-se $O+Q$ igual a Q, ou seja, O é o elemento de identidade aditiva (o elemento zero) do grupo de pontos;
(2) Se P não é um ponto no infinito, $-P$ é ponto com o mesmo valor para a coordenada x, porém com o valor negativo para a coordenada y, ou seja, $-(x, y) = (x, -y)$. Observando a curva E (equação 24), é possível perceber que se (x, y) é um ponto da curva, o ponto $(x, -y)$ também será. Se $Q = -P$, então defini-se que $P + Q$ será o ponto no infinito O.
(3) Se P e Q tem coordenada x diferentes, uma reta traçada entre os ponto P e Q intercepta a curva E em um terceiro ponto R. Então, define-se que a adição de $P + Q$ será igual ao ponto $-R$, o qual é o ponto espelhado de R com relação ao eixo x (ver Figura 2).
(4) Se $P = Q$, então a reta entre os ponto P e Q será uma reta tangente a curva E no ponto P. Seja R o outro ponto da interceptação entre reta com a curva E, pode-se definir $2P = -R$ (ver Figura 3).

Seja (x_p, y_p), (x_q, y_q) e (x_r, y_r) as coordenadas dos pontos P, Q e R, respectivamente. As coordenadas x_r e y_r podem ser obtidas em função das coordenadas x_p, y_p, x_q, y_q.

Considere que $P \neq Q$ e que a equação da reta que passa pelos pontos P e Q seja

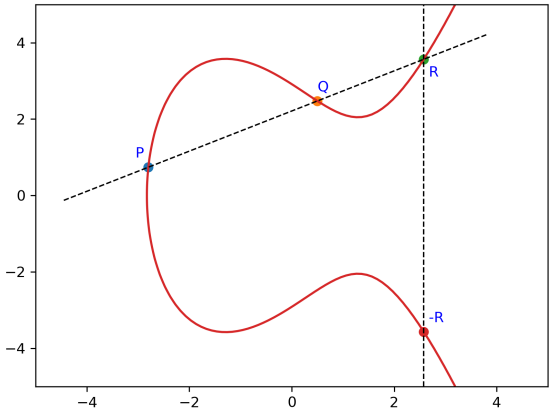

Figura 2. Ilustração da adição de ponto em uma curva elíptica para o caso $P+Q$ com coordenada x diferentes para os pontos P e Q.

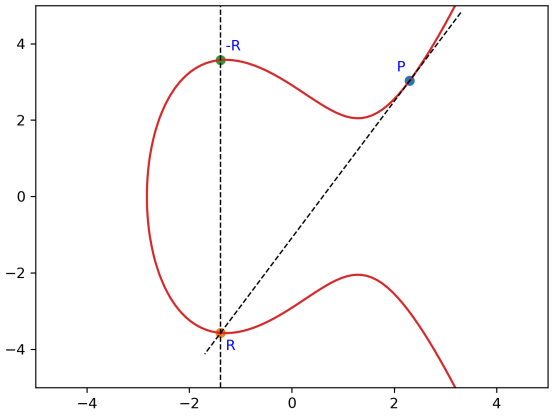

Figura 3. Ilustração da adição de ponto em uma curva elíptica para o caso $P = Q$.

$$y = \alpha x + \beta, \tag{25}$$

então tem-se que

$$\alpha = \frac{y_q - y_p}{x_q - x_p} \tag{26}$$

e

$$\beta = y_p - \alpha x_p. \tag{27}$$

Um ponto $(x, \alpha x + \beta)$ pertence a curva elíptica E se e somente se

$$(\alpha x + \beta)^2 = x^3 + ax + b. \tag{28}$$

Assim, há um ponto de interseção para cada raiz da equação cúbica dada por

$$x^3 - (\alpha x + \beta)^2 + ax + b. \tag{29}$$

Como já se conhecem duas destas raízes $(x_p, \alpha x_p + \beta)$ e $(x_q, \alpha x_q + \beta)$, que são os pontos P e Q na curva, a terceira raiz poderá ser obtida expandido-se (29) e aplicando-se (12), ou seja

$$\alpha^2 = x_p + x_q + x_r. \tag{30}$$

Desta forma, as coordenadas de R serão $(x_r, (\alpha x_r + \beta))$ e são calculadas da seguinte forma:

$$\begin{aligned} x_r &= \alpha^2 - x_p - x_q, \\ y_r &= y_p - \alpha(x_p - x_r), \end{aligned} \tag{31}$$

e consequentemente, o ponto $P + Q = -R$ terá as coordenadas dadas por $(x_r, -y_r)$.

Considere que $P = Q$ e que a equação da reta que passa pelos pontos P e Q seja

$$y = \alpha_2 x + \beta, \tag{32}$$

em que β é o mesmo da equação (27) e α_2 é a derivada da curva no ponto P, ou seja,

$$\alpha_2 = \frac{dy}{dx} = \frac{3x_p^2 + a}{2y_p}. \tag{33}$$

Desta forma, as coordenadas de R para este caso serão $(x_r, (\alpha x_r + \beta))$ e são calculadas da seguinte forma:

$$\begin{aligned} x_r &= \alpha_2^2 - 2x_p, \\ y_r &= y_p - \alpha_2(x_p - x_r), \end{aligned} \tag{34}$$

e consequentemente, o ponto $2P = -R$ terá as coordenadas dadas por $(x_r, -y_r)$.

A adição de pontos na curva elíptica sobre os números reais é uma boa abordagem para ver as etapas subjacentes na execução da operação. No entanto, os cálculos provam ser lentos e imprecisos devido a erros de arredondamento, e a implementação desses cálculos em esquemas criptográficos requer aritmética rápida e precisa. Portanto, grupos de curvas elípticas sobre corpos finitos como $\mathbb{F}_n$, quando $n > 3$ é primo, são usados na prática (O'Maley, 2004).

Uma curva elíptica com $\mathbb{F}_n$ como corpo subjacente pode ser formada escolhendo-se a e b dentro do corpo $\mathbb{F}_n$. Semelhante ao caso dos números reais, a curva inclui todos os pontos (x, y) em $\mathbb{F}_n \times \mathbb{F}_n$ que satisfazem a equação da curva elíptica

$$y^2 \equiv x^3 + ax + b \pmod{n}, \tag{35}$$

em que $x, y \in \mathbb{F}_n$. Assim como no caso dos números reais, se

$$-(4a^3 + 27b^2) \not\equiv 0 \pmod{n}, \tag{36}$$

a curva elíptica forma um grupo, o qual consiste de pontos na curva, juntamente com o O. Definindo-se o ponto negativo de um ponto $P = (x_p, y_p)$ como

$$-P = (x_p, -y_p \pmod{n}). \tag{37}$$

A aritmética no grupo da curva elíptica sobre $\mathbb{F}_n$ é semelhante ao caso dos números reais, sendo a diferença que todo os cálculos são realizados sobre a aritmética modular. Desta forma, as equações (31,34) são ajustadas para

$$\begin{aligned} x_r &\equiv \alpha^2 - x_p - x_q \pmod{n}, \\ y_r &\equiv y_p - \alpha(x_p - x_r) \pmod{n}, \\ x_r &\equiv \alpha_2^2 - 2x_p \pmod{n}, \\ y_r &\equiv y_p - \alpha_2(x_p - x_r) \pmod{n}, \end{aligned} \tag{38}$$

respectivamente.

5. RESULTADOS

O objetivo desta seção é apresentar o resultado da comparação dos tempo de processamento, na codificação e decodificação, dos sistemas criptográficos RSA e ECC para uma garantia de nível de segurança semelhante. O método RSA necessita de chaves maiores para equiparar-se a modelos com função logarítmica e até criptografias simétricas. Mantendo o mesmo nível de segurança, uma chave de 1024

bit em RSA equipara-se a uma chave de apenas 160 **bit** em ECC (Suárez-Albela et al., 2018). A Tabela 1 retirada de Gupta et al. (2002) compara os tamanhos de chaves para o mesmo nível de segurança em diferentes métodos.

Tabela 1. Tamanho de Chaves de Seguranças Equivalentes

Simétrico	ECC	RSA/DH/DSA
80	163	1024
128	283	3072
192	409	7680
256	571	15360

A comparação entre os sistemas criptográficos foi realizada em um sistema operacional baseado em **Linux** (Ubuntu 22.04.2 LTS), com o processador Intel Core i7-4702HQ (2.20 GHz) e ambos os programas foram desenvolvidos em C++. Foram testados diferentes tamanhos de chaves e calculado os tempos de codificação e decodificação da mensagem. A Tabela 2 ilustra o comparativo das performances.

Tabela 2. Comparativo dos algoritmos ECC e RSA.

Método	Chave (bits)	Codificação (s)	Decodificação (s)
ECC	160	0.948	1.257
RSA	1024	2.571	2.916
ECC	224	1.325	1.853
RSA	2048	9.859	10.173
ECC	256	1.947	2.260
RSA	3072	35.964	37.057
ECC	272	2.376	2.806
RSA	4096	71.642	73.951

6. CONCLUSÕES

Aplicar alguma técnica de criptografia na troca de informação é amplamente utilizada por proporcionar de maneira prática e eficiente uma proteção contra ataques. No cenário atual, com a grande expansão de dispositivos IoT, faz-se necessário a busca por novas implementações das técnicas de criptografia, porém que sejam mais leves para evitar gastos excessivos de energia. Como visto ao longo deste trabalho, a ECC consegue garantir o mesmo nível de segurança da RSA, porém com chaves menores, o que impacta diretamente no tempo de processamento e, consequentemente, no consumo energético.

Muitas aplicações de IoT podem requerer a implementação de comunicação em microcontroladores com CPUs (*Central Processing Unit*) bem limitadas, o que torna desafiador a implementação de sistemas criptográficos. Este trabalhou iniciou os estudos para o desenvolvimento de uma implementação de criptografia de curva elíptica leve, ou seja, que demande chaves menores para reduzir as exigências do microcontrolador. Para manter a segurança com chaves menores, associa-se a criptografia uma autenticação baseada em atributos inserindo uma segunda camada de proteção, que em conjunto com o ECC leve possam garantir a segurança na comunicação do dispositivo IoT.

AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

REFERÊNCIAS

Bhardwaj, I., Kumar, A., e Bansal, M. (2017). A review on lightweight cryptography algorithms for data security and authentication in iots. In *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*, 504–509. doi:10.1109/ISPCC.2017.8269731.

Buchanan, W. e Woodward, A. (2017). Will quantum computers be the end of public key encryption? *Journal of Cyber Security Technology*, 1(1), 1–22. doi:10.1080/23742917.2016.1226650.

Carracedo, J.M., Milliken, M., Chouhan, P.K., Scotney, B., Lin, Z., Sajjad, A., e Shackleton, M. (2018). Cryptography for security in iot. In *2018 Fifth International Conference on Internet of Things: Systems, Management and Security*, 23–30. doi:10.1109/IoTSMS.2018.8554634.

Gupta, V., Gupta, S., Chang, S., e Stebila, D. (2002). Performance analysis of elliptic curve cryptography for ssl. In *Proceedings of the 1st ACM Workshop on Wireless Security*, WiSE '02, 87–94. Association for Computing Machinery, New York, NY, USA. doi:10.1145/570681.570691.

Hassan, R. e Qamar, T. (2010). Asymmetric-key cryptography for contiki.

Koblitz, N., Menezes, A., Wu, Y., e Zuccherato, R. (2004). *Algebraic Aspects of Cryptography*. Algorithms and Computation in Mathematics. Springer Berlin Heidelberg.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, 48(177), 203–209.

Miller, V.S. (1985). Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques*, 417–426. Springer.

Mosenia, A. e Jha, N.K. (2017). A comprehensive study of security of internet-of-things. *IEEE Transactions on Emerging Topics in Computing*, 5(4), 586–602. doi:10.1109/TETC.2016.2606384.

O'Maley, A. (2004). Elliptic curves and elliptic curve cryptography.

Rivest, R.L., Shamir, A., e Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2), 120–126. doi:10.1145/359340.359342.

Statista, R.D. (2022). Number of internet of things (iot) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030. URL `http://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/`.

Suárez-Albela, M., Fernández-Caramés, T.M., Fraga-Lamas, P., e Castedo, L. (2018). A practical performance comparison of ecc and rsa for resource-constrained iot devices. In *2018 Global Internet of Things Summit (GIoTS)*, 1–6. doi:10.1109/GIOTS.2018.8534575.