# INVESTIGAÇÃO DE ALGORITMOS DE CRIPTOGRAFIA UTILIZANDO CURVAS ELÍPTICAS

GUSTAVO ADOLFO SCHWANTZ OLIVEIRA[1]; RAFAEL IANKOWSKI SOARES[2]

[1]*Universidade Federal de Pelotas (UFPel) – gasoliveira@inf.ufpel.edu.br*
[2]*Universidade Federal de Pelotas (UFPel) – rafael.soares@inf.ufpel.edu.br*

## 1. INTRODUÇÃO

A criptografia de chave pública (PKC), ou criptografia assimétrica, é uma ferramenta indispensável na atual era da informação. Ela se difere da criptografia simétrica no fato de usar chaves distintas nos processos de encriptação e decriptação. Suas aplicações vão desde a ocultação de dados a assinaturas digitais e distribuição de chaves criptográficas (PAAR; PELZL, 2010).

Todo algoritmo de chave pública baseia a sua segurança em um problema matemático difícil de resolver. O RSA (Rivest-Shamir-Adleman) (RIVEST; SHAMIR; ADLEMAN, 1978), o algoritmo mais usado do gênero, é baseado na dificuldade de se fatorar números inteiros. Já a troca de chaves Diffie-Hellman (DHKE) (DIFFIE; HELLMAN, 1976) depende a sua segurança na dificuldade de se resolver o problema do logaritmo discreto (DLP). O DLP é o problema em que, dado um valor $\alpha$ e outro $\beta$, é preciso encontrar um valor inteiro $x$ tal que $\alpha^x = \beta$.

É importante observar que os problemas matemáticos citados só fornecem segurança para os respectivos algoritmos se os operandos envolvidos forem números muito grandes (acima de 1024 bits). Isso faz com os algoritmos de chave pública sejam computacionalmente intensivos, usando muita memória e processamento.

Em 1985, Victor Miller (MILLER, 1985), e logo em seguida em 1987 Neal Koblitz (KOBLITZ, 1987), propuseram, de maneira independente, o uso de curvas elípticas no DLP dando origem a criptografia com curvas elípticas (ECC). Uma curva elíptica é definida mediante equações cúbicas na forma

$$y^2 = x^3 + ax + b.$$

A grande vantagem da ECC é que ela fornece um nível de segurança igual ao RSA e a DHKE usando operandos de tamanho muito inferior: uma chave ECC de 128 bits é equivalente a uma chave de 1024 bits RSA. Isso faz com que implementações ECC sejam mais eficientes que a de outros algoritmos de chave pública, tornando-a um atrativo para dispositivos embarcados (REDDY at al., 2016) e Internet das Coisas (IoT) (HE; ZEADALLY, 2015).

Este trabalho é baseado em um projeto de conclusão de curso que está em andamento e possui dois objetivos principais. O primeiro deles é apresentar uma revisão sobre curvas elípticas, mostrando suas operações e como elas podem ser usadas para montar uma primitiva criptográfica. O segundo é revisar os principais algoritmos usados em ataques contra PKC, inclusive contra ECC. Entender o poder destes ataques nos dão um entendimento do porquê a ECC possuir chaves de menor tamanho.

## 2. METODOLOGIA

Para alcançar o primeiro objetivo deste trabalho, foi feito um estudo aprofundado a respeito de criptografia e PKC, além dos fundamentos matemáticos nos quais a criptologia é baseada. Foram revisados os conceitos de função de mão única, aritmética modular, corpos finitos, grupos cíclicos, etc, (PAAR; PELZL, 2010), (COHEN; FREY, 2006). Em seguida, buscou-se entender o que são curvas elípticas, suas operações (adição de ponto, multiplicação de ponto) e como elas se aplicam na PKC (BLAKE; SEROUSSI; SMART, 2005).

O segundo objetivo do trabalho foi alcançado revisando-se os modelos de ataque existentes contra a PKC, tais como os métodos *Baby-step giant-step* e *Rho de Pollard.* Para isso, usou-se (MENEZES; OORSCHOT; VANSTONE, 1996). A razão de se analisar estes métodos é que eles fornecem a explicação para a maior segurança da ECC e suas vantagens em relação a outras primitivas.

## 3. RESULTADOS E DISCUSSÃO

Este trabalho procurou entender o que são curvas elípticas e como elas podem ser usadas no DLP para construir primitivas criptográficas. Foram revisados algoritmos de ataque como *Método da Força Bruta, Baby-step giant-step* e *Rho de Pollard.* O estudo destes métodos e como eles se aplicam a PKC forneceram o entendimento do porquê a ECC ser mais eficiente que primitivas alternativas. A Tabela 1 abaixo compara os diferentes tamanhos de chave da ECC com o tamanho de chaves equivalentes de outros algoritmos de chave pública.

**Tabela 1. Tamanho dos operandos para diferentes algoritmos (em bits)**

| ECC | RSA | DHKE |
|---|---|---|
| 160 | 1024 | 1024 |
| 256 | 3072 | 3072 |
| 384 | 7680 | 7680 |
| 512 | 15360 | 15360 |

Como dito na Seção 1, este trabalho ainda se encontra em andamento. Na sua próxima etapa, o autor pretende implementar os algoritmos descritos anteriormente em primitivas ECC, RSA e DHKE, comparando os resultados. Com isso, espera-se corroborar as conclusões obtidas com o estudo teórico.

## 4. CONCLUSÕES

Este trabalho traz como inovação um estudo detalhado da ECC e mostra as suas vantagens em relação a outros esquemas criptográficos, disponibilizando resultados práticos que serão obtidos obedecendo o rigor científico e poderão ser usados futuramente por outros pesquisadores interessados em PKC.

O trabalho inova no sentido de comparar de maneira específica a ECC com algoritmos assimétricos já consolidados na criptografia, não só em termos de desempenho, mas também realiza uma avaliação quantitativa da vulnerabilidade a certos ataques.

## 5. REFERÊNCIAS BIBLIOGRÁFICAS

PAAR, C.; PELZL, J. **Understanding Cryptography: A Textbook for Students and Practitioners**. Berlin: Springer, 2010. 1v.

BLAKE, I. F.; SEROUSSI, G.; SMART, N. P. **Advances in Elliptic Curve Cryptography (London Mathematical Society Lecture Note Series)**. United kingdom: Cambridge University Press, 2005. 2v.

MENEZES, A. J.; OORSCHOT, P. C. van; VANSTONE, S. A. **Handbook of Applied Cryptography**. New York: CRC Press, 1996. 1v.

COHEN, H.; FREY G. **Handbook of Elliptic and Hyperelliptic Curve Cryptography**. USA: Chapman & Hall/CRC, 2006. 1v.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. **Communications of the ACM**, New York, v.21, n.2, p.120-126, 1978.

KOBLITZ, N. Elliptic Curve Cryptosystems. **Math. Comp.**, USA, v.48, n.1, p.203-209, 1987.

DIFFIE, W.; HELLMAN, M. New Directions in Cryptography. **IEEE Transactions on Information Theory**, USA, v.22, n.6, p.644-654, 1976.

MILLER, V. S. Use of Elliptic Curves in Cryptography. **Annual International Cryptology Conference**, USA, p.417-426, 1985.

HE, D.; ZEADALLY, S. An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography. **IEEE Internet of Things Journal**, USA, v.2, n.1, p.72-83, 2015.

REDDY, A. G.; DAS, A. K.; YOON, E.; YOO, K. A Secure Anonymous Authentication Protocol for Mobile Services on Elliptic Curve Cryptography. **IEEE Acess**, USA, v.4, p.4394-4407, 2016.