MO422 - Algorítmos Critptográficos
2º Semestre 2024
Prof: Julio Lopez
Aluno: Guilherme Augusto Amorim Terrell

Proposta de trabalho: Estudo de algoritmos para compartilhamento de segredos

Introdução
Dentro do contexto de criptografia simétrica um dos grandes desafios é prover um meio seguro para o compartilhamento da chave privada através de um canal sabidamente inseguro. No contexto de sistemas embarcados, para além do compartilhamento seguro também se faz necessário o uso de algorítmos eficientes, capazes de prover a segurança necessária consumindo o mínimo possível de recursos como memória, tempo de processamento e energia, dessa forma, existem muitas aplicações de compartilhamento de chave em sistemas embarcados que utilizam algorítmos de curvas elípticas, uma vez que os mesmos conseguem prover alto nível de segurança com uma chave de tamanho menor do que outros algorítmos como RSA.

Objetivos
Estudar em detalhes o algorítmo curve25519 para troca de chave, visando entender e explorar o seu uso no contexto de sistemas embarcados, destacando as principais diferenças em relação ao algorítmo RSA (que não é baseado em curvas elípticas e que também é bastante utilizado para troca de chaves em sistemas embarcados).

Metodologia
O trabalho será pautado no estudo sistemático de livros, artigos e de implementações em códigos aberto do algorítmo curve25519 para troca de chave. Propõe-se também como prova de conceito uma análise quantitativa (ex: consumo de memória, tempo de execução) comparando o curve25519 com o RSA.

Referências bibliográficas

1. HAYATO, Fujii., ARANHA, Diego. “Curve25519 for the Cortex-M4 and beyond”. Disponível em https://www.lasca.ic.unicamp.br/media/publications/paper39.pdf
2. HAYATO, Fujii., ARANHA, Diego. “Efficient Curve25519 Implementation for ARM Microcontrollers”. Disponível em https://sol.sbc.org.br/index.php/sbseg_estendido/article/view/4142/4071
3. MICROCHIP. “RSA vs. ECC comparison for Embedded Systems”. Disponível em https://ww1.microchip.com/downloads/en/DeviceDoc/00003442A.pdf
4. STALLINGS, William. Other Public Key Cryptosystems. *In*: STALLINGS, William. Cryptography and Network Security Principles and Practice. England: PEARSON, 2017.p.313- 336.

Outras referências podem ser utilizadas ao longo dos estudos.