Estudo de Algoritmos Criptográficos Simétricos na Placa Beaglebone Black

Bruno A. da Silva, Iago S. Ochôa, Valderi R.Q. Leithardt

[1]Universidade do Vale do Itajaí (UNIVALI), Itajaí, Brasil, 88302-901
Laboratório de Sistemas Embarcados e Distribuídos

{silvabruno, iago.ochoa}@edu.univali.br, valderi@univali.br

Resumo. *Neste artigo é realizada uma análise de desempenho dos algoritmos criptográficos de chave simétrica, Advanced Encryption Standard (AES) e Rivest Cipher 6 (RC6), implementados na placa Beaglebone Black com diferentes tamanhos de pacote e chave. Com a realização dos testes, foi possível perceber que o algoritmo RC6 obteve melhor desempenho em relação ao AES.*

Palavras-Chave: *Criptografia, Algoritmos, Segurança, Privacidade de Dados;*

1. Introdução

Segundo [Naru et al. 2017], a Internet das Coisas (IoT - Internet of Things) está cada vez mais presente no cotidiano das pessoas, como na medicina, em redes elétricas inteligentes (Smart Grids), automação residencial, agricultura e mobilidade urbana. Com isto surge a necessidade de proteger os dados processados pelos dispositivos IoT contra *hackers* e invasores. Um modo de resolver este problema é através de algoritmos criptográficos, em contrapartida criptografias demandam muito poder computacional. Sistemas embarcados possuem poder computacional limitado, assim, o desempenho de algoritmos criptográficos é bem menor, gerando tempo de execução maior.

O AES, originalmente chamado Rijndael, foi desenvolvido na década de 1990 por Vincent Rijmen e Joan Daemen para participar do concurso que substituiria o algoritmo criptográfico padrão do governo dos Estados Unidos, o DES, que já estava inseguro [William 2006]. O algoritmo Rijndael acabou sendo escolhido como o melhor algoritmo do concurso e a partir de então passou a chamar-se AES [Daemen and Rijmen 2013].

Desde sua criação, já foram realizadas várias modificações no algoritmo original e ataques específicos quebraram apenas algumas rodadas da criptografia [Biham et al. 2005]. O AES possui quatro etapas de transformação, sendo elas: SubBytes, ShiftRows, AddRoundKey e MixColumns, cada uma indispensável para a segurança do algoritmo.

O RC6 é um algoritmo derivado do RC5, e desenvolvido por Ron Rivest, Matt Robshaw, Ray Sidney e Yiqun Lisa Yin. Foi concorrente do Rijndael no concurso para o Advanced Encryption Standard, onde foi derrotado pois além de necessitar de uma quantidade grande de memória, seu desempenho em FPGA (Field Programmable Gate Array) não foi satisfatório [Daemen and Rijmen 2013]. Assim, possui desempenho superior em software do que em hardware se comparado a outros algoritmos criptográficos, em Linguagem C foi o algoritmo mais rápido entre os concorrentes [Soewito et al. 2016]. O

algoritmo é baseado na cifra de Feistel, com entrada de texto pleno de 128 bits dividido em 4 entradas de 32 bits e tamanho de chave de até 256 bits.

O RC6 é um algoritmo simples de compreender e menos complexo que o AES, que possui várias etapas baseadas em princípios algébricos sofisticados. Como tem base na cifra de Feistel, o RC6 conta com muitas operações de rotação de bits, XOR e rotação de posições das entradas. Outros exemplos de criptografias baseadas em cifra de Feistel são: Blowfish, CAST, DES e 3DES.

Portanto, o principal objetivo deste trabalho é analisar, considerando tamanhos de pacotes e chaves variados, os algoritmos de chave simétrica AES e RC6 na placa Beaglebone Black em continuação aos trabalhos desenvolvidos em [da Silva et al. 2018]. No trabalho de [Ochôa et al. 2018], foram realizados testes com os algoritmos RC6, AES (128, 192 e 256) e 3DES no microcontrolador MSP430F6749. As criptografias que obtiveram melhor resultado foram o AES e o RC6, por este motivo foram escolhidos estes algoritmos inicialmente.

2. Testes Realizados

Todos os testes foram realizados na placa BeagleBone Black, que possui 512MB de RAM DDR3 e uma CPU ARM Cortex A8 AM3358 com um núcleo operando a 1GHz. Além disso, foi utilizado o sistema operacional Debian 9.4 em um cartão SD de 16GB.

Foram medidos os tempos de encriptação e decriptação de pacotes de dados com tamanhos de 128KB, 256KB, 512KB e 1024KB baseando-se no trabalho de [Silva et al. 2018], juntamente com chaves de 128, 192 e 256 bits nos algoritmos RC6 e AES, ambos utilizando a cifra de bloco ECB (Electronic Codebook) e implementados em Linguagem C.

Na Tabela 1 são demonstrados os tempos de encriptação em todas as três chaves para tamanhos de pacotes testados. Todos os tempos foram obtidos realizando a média aritmética de dez testes consecutivos em milissegundos para maior precisão nos resultados atingidos. Pode-se perceber que o tamanho de chave afetou aproximadamente 1% do tempo total e, em média, o tempo dobrou conforme eram dobrados os tamanhos dos pacotes, tanto para o AES quanto para o RC6, demonstrando um crescimento linear.

Tamanho	**128bits**		**192bits**		**256bits**	
Pacote/Chave	**AES**	**RC6**	**AES**	**RC6**	**AES**	**RC6**
128KB	509	71	509	71	512	71
256KB	1019	138	1017	140	1042	142
512KB	2049	275	2033	277	2043	277
1024KB	4110	551	4105	553	4138	552

Tabela 1. Tempos (ms) de encriptação considerando tamanhos de pacote e chave

A Tabela 2 demonstra os tempos de execução obtidos na decriptação dos quatro pacotes testados com as três chaves, também medidos em milissegundos. Neste caso o AES obteve tempos de decriptação maiores do que encriptação e o RC6 obteve tempos melhores do que sua etapa de encriptação. O impacto das chaves em ambos os algoritmos afetou menos de 1% do desempenho total. Em dispositivos ainda mais limitados,

como utilizado por [Ochôa et al. 2018], a diferença de tempo entre as chaves são mais expressivas, contribuindo também com resultados para uso em IoT.

Tamanho Pacote/Chave	128bits		192bits		256bits	
	AES	RC6	AES	RC6	AES	RC6
128KB	602	67	601	68	607	68
256KB	1208	133	1203	137	1213	138
512KB	2418	269	2411	273	2423	269
1024KB	4840	533	4814	547	4866	533

Tabela 2. Tempos (ms) de decriptação considerando tamanhos de pacote e chave

Na Figura 1 evidencia a diferença entre o algoritmo RC6 em relação ao AES. Durante os testes realizados foi possível perceber que o RC6 possui menos etapas e operações mais simples que o AES, isto pode explicar seu desempenho superior nas condições testadas.

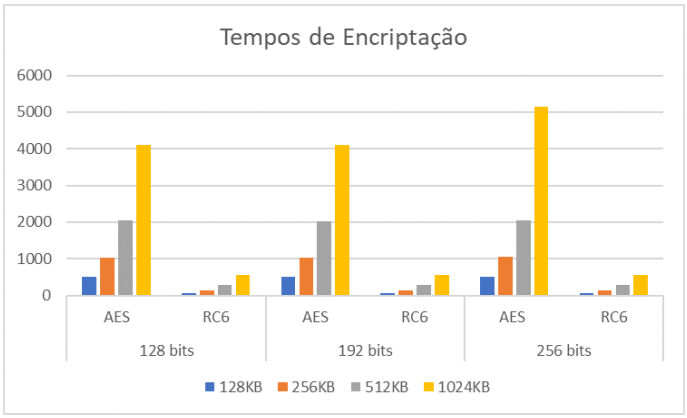

Figura 1. Gráfico comparativo entre os tempos de encriptação.

A Figura 2 demonstra que, em todos os casos abordados, o RC6 obteve tempos menores para decriptar os pacotes do que para encriptar, enquanto o AES demorou mais tempo para decriptação do que encriptação. Entretanto, não foi possível concluir o porquê.

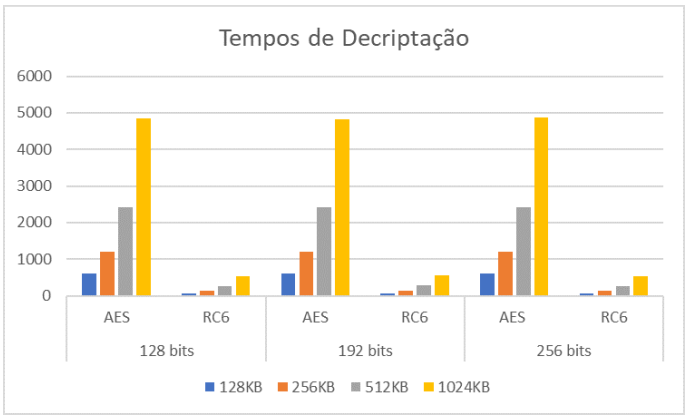

Figura 2. Gráfico comparativo entre os tempos de decriptação.

3. Conclusões e Trabalhos Futuros

Nos testes e análise dos resultados preliminares obtidos, foi possível observar que o RC6 demonstra desempenho superior ao AES nos casos testados, obtendo desempenho de oito a dez vezes superior. Sendo relevante para uso em casos em que o tempo de processamento precisa ser o mais baixo possível, como em comunicações. Com isso, foi possível concluir que o RC6 possui maior viabilidade de uso devido aos seus tempos melhores em relação ao AES, sendo importante ressaltar que não foi utilizado o acelerador criptográfico presente no Beaglebone Black, pois o objetivo do trabalho é avaliar os desempenhos dos algoritmos sob o mesmo ambiente, sem nenhum tipo de otimização ou aceleração externa ao CPU principal do ARM.

Em trabalhos futuros pretende-se desenvolver otimizações para ambos os algoritmos para melhor desempenho, análise de uso de memória, testes com outros algoritmos criptográficos, testes em diferentes microcontroladores e aplicações em contextos e cenários específicos.

4. Agradecimentos

Este trabalho foi financiado pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) - Código Financeiro 001.Também agradecemos o uso da infraestrutura fornecida pelo Laboratório de Sistemas Embarcados e Distribuídos (LEDS) da UNIVALI.

Referências

Biham, E., Dunkelman, O., and Keller, N. (2005). Related-key boomerang and rectangle attacks. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 507–525. Springer.

da Silva, B. A., de Mello, G., Silva, L. A., and Leithardt, V. R. Q. (2018). Comparative study of aes cryptographic algorithm in limited capacity device. *Workshop em Sistemas de Informação do IFC*, 1.

Daemen, J. and Rijmen, V. (2013). *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media.

Naru, E. R., Saini, H., and Sharma, M. (2017). A recent review on lightweight cryptography in iot. In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pages 887–890.

Ochôa, I. S., Teive, R. C., Alonso, E. E., and Leithardt, V. R. (2018). Uma análise de desempenho criptográfico de algoritmos implementados no microcontrolador msp430f6749 utilizando o protocolo osgp. *Anais SULCOMP*, 9.

Silva, L. A., Leithardt, V. R. Q., Dazzi, R. S., and Silva, J. S. (2018). PRISER - Utilização de BLE para localização e notificação com base na privacidade de dados. *Rev*, v.2(Speci).

Soewito, B., Gunawan, F. E., Diana, and Antonyová, A. (2016). Power consumption for security on mobile devices. In *2016 11th International Conference on Knowledge, Information and Creativity Support Systems (KICSS)*, pages 1–4.

William, S. (2006). *Cryptography and network security: principles and practices*. Pearson Education India.