Extração de Dados do Mapeamento Sistemático

Tema de pesquisa:Análise de confiabilidade dos algoritmos de criptografia.

Giulio Emmanuel da Cruz Di Gerolamo
790965

Seleção dos Estudos Relevantes

A partir da seleção feita na etapa 1 da seleção feita no mapeamento sistemático do Tópico 4, que foi realizada a partir das 3 strings: [Algoritmo] + [Criptografia] + [Velocidade].
A partir dessa busca foram encontrados 6 resultados. A maioria dos artigos encontrados não estão presentes no Qualis CAPES. Então, para encontrar o artigo qualificado no Qualis CAPES foi feita a busca em Inglês das mesmas chaves traduzidas.

Artigo	**Idioma**	**Linguagem**	**Nome da criptografia**	**Tipo de criptografia**	**Ano da publicação**
Artigo A	Inglês	C	RSA	Chave de inteiros	2012
Artigo B	Português	C	Grover e Shor	Fatoração quântica	2020
Artigo C	Inglês	C	CRYSTALS-Kyber	Chave quântica	2021

Fichamento do Artigo C

1. **Dados bibliográficos:**
    a. Assunto:
    Aceleração de algoritmos de criptografia pós-quântica em um processador RISC-V através da introdução de uma Unidade de Lógica Aritmética dedicada
    b. Título:
    A RISC-V Post Quantum Cryptography Instruction Set Extension for Number Theoretic Transform to Speed-Up CRYSTALS Algorithms
    ou em português:
    Uma Extensão de Conjunto de Instruções RISC-V para Criptografia Pós-Quântica com Transformada Numérica para Acelerar os Algoritmos CRYSTALS
    c. Base de dados:
    Periódicos da CAPES
    d. Referência:
    P. Nannipieri, S. Di Matteo, L. Zulberti, F. Albicocchi, S. Saponara and L. Fanucci, "A RISC-V Post Quantum Cryptography Instruction Set Extension for Number Theoretic Transform to Speed-Up CRYSTALS Algorithms," in IEEE Access, vol. 9, pp. 150798-150808, 2021, doi: 10.1109/ACCESS.2021.3126208. Recuperado de: https://ieeexplore.ieee.org/document/9605604/citations#citations
2. **Dados de conteúdo:**
    a. Resumo:
    A criptografia de chave pública é essencial para infraestruturas digitais, mas enfrenta ameaças de computadores quânticos. A criptografia pós-quântica busca algoritmos resistentes a ataques quânticos. O NIST seleciona candidatos, como construções criptográficas baseadas em retículas. Para acelerar esses algoritmos, uma solução é incorporar uma Unidade de Lógica Aritmética pós-quântica em um processador RISC-V, proporcionando maior velocidade e economia de energia.
3. **Respostas a questões de pesquisa:**
    a. Qual o impacto da velocidade na segurança de uma criptografia?
    A velocidade, por se tratar de computação quântica, não alterou a segurança da criptografia.
    b. Quais consequências a o método utilizado traz para a segurança de dados?
    Por se tratar de computação quântica, a qual tem facilidade maior de quebrar criptografia comum, é necessário uma criptografia também quântica.

4. **Respostas a questões gerais:**
    a. O que foi obtido como resultado desse trabalho?
    Combinando os resultados alcançados em termos de complexidade, desempenho de tempo e energia por função, o que observamos é que com nossa solução conseguimos um aumento de velocidade de 20% a 65% nas Funções Kyber e Dilithium, com um aumento quase insignificante de LUT (+3%), sem impacto nos FF e uso moderado de DSP (+5 unidades) na FPGA.
    b. Como esse trabalho se relaciona com outros da mesma área?
    Trás uma abordagem diferente com a computação quântica, agregando mais características da mesma a criptografia.
    c. Qual seria o próximo passo razoável para dar continuidade a essa pesquisa?
    Encontrar novos meios de obter ganhos nos algoritmos com o mínimo de perda de desempenho.

Fichamento do Artigo A

5. **Dados bibliográficos:**
    a. Assunto:
    Abordar a relação existente entre a busca pela segurança de dados e a velocidade de codificação e decodificação do algoritmo de criptografia RSA
    b. Título:
    Algoritmo de criptografia RSA: análise entre a segurança e velocidade
    c. Base de dados:
    Periódicos da CAPES
    d. Referência:
    Rafael Santos de Andrade, Fernando dos Santos Silva, "Algoritmo de criptografia RSA: análise entre a segurança e velocidade" in Eventos Pedagógicos, 2012, Vol.3 (3), p.438-457. Recuperado de: https://sinop.unemat.br/projetos/revista/index.php/eventos

Fichamento do Artigo B

6. **Dados bibliográficos:**
    a. Assunto:
    Apresentar os algoritmos quânticos de Grover e Shor, amplamente utilizados na computação quântica, com uma proposta original focada nos estados quânticos obtidos após cada passo na evolução do circuito.
    b. Título:

Um estudo passo a passo dos algoritmos de Grover e Shor

c. Base de dados:
   Periódicos da CAPES
d. Referência:
   Luciano Alves Vieira, Clarice Dias de Albuquerque, "Um estudo passo a passo dos algoritmos de Grover e Shor" in DOAJ Directory of Open Access Journals,C.Q.D., 2020, Vol.19. Recuperado de: http://www2.fc.unesp.br/#!/revistacqd/