Relatório ISL

Diogo Tuler Chaves, João Marcos Tomáz, Rafael Martins Gomes
Universidade Federal de Minas Gerais (UFMG)
Belo Horizonte - MG - Brasil

1 - Introdução

Com a entrada da era tecnológica, foram sendo desenvolvidas formas de análises de dados cada vez mais eficientes, como forma de resoluções de problemas e estudos para melhorar a vida humana. Com isso,preocupações como a segurança de dados vieram à tona, assim a criptografia ganhou forte espaço no cenário. Uma dessas técnicas é a criptografia digital, que consiste em transformar informações em códigos para evitar o acesso de pessoas não autorizadas ao conteúdo da mensagem.Maneiras de se manter seguras as informações são pautas importantes nos dias atuais, o trabalho abaixo consiste em demonstrar algumas formas relevantes.

O método aqui demonstrado chama-se One Time Pad (OTP), um estilo de criptografia praticamente inquebrável. A criptografia inquebrável está disponível desde 1920. Ela deriva da cifra de Vernam . No entanto, não conseguindo resolver os problemas de distribuição de chaves da criptografia única, os criptologistas recorreram à criptografia de chave pública na década de 1970 para compartilhar chaves secretas curtas de algoritmos simétricos. As mensagens cifradas com OTP não fornecem nenhuma informação sobre a mensagem original a um criptoanalista e sua segurança foi provada matematicamente por Claude Shannon durante a 2ª Guerra Mundial. Historicamente, o OTP foi usado por várias nações para trafegar informações sigilosas, seja em comunicações feitas por espiões ou troca de informações confidenciais durante guerras.

Neste trabalho, também apresenta-se a implementação e execução de um Linear Feedback Shift Register (LFSR). Ele consiste em um gerador pseudo-aleatório de números binários, podendo ser muito útil para se obter a segurança das informações. Para sua implementação, foi utilizado um código em Verilog, que consiste numa HDL (Hardware Description Language) utilizada para desenvolvimento de hardwares. Esse registrador utiliza uma porta XOR para obter os bits mais significativos das de suas saídas a partir do que chamamos de feedback.

Esses números binários são importantes pois eles podem gerar uma chave que será útil para criptografar uma informação. Essa chave, ao se juntar a dado, impede que ele seja facilmente reconhecido, tornando-o seguro.

O uso de tais métodos e tecnologias é crucial na implementação de cifradores com hardware. Para isso, deve-se fazer a análise da arquitetura geral do cifrador e do que será necessário para desenvolvê-lo, bem como o projeto do circuito a ser utilizado. Essas etapas envolvem a decisão de qual método de criptografia será utilizado, como o OTP, e de quais operações o circuito irá realizar, como o deslocamento linear implementado neste trabalho. A fim de verificar de modo inteligível como o circuito funcionará e será projetado, faz-se uso de linguagens de descrição de hardware, como Verilog. Com o código feito, é possível compreender o comportamento do circuito de forma clara e realizar testes para checar se os componentes funcionam com diferentes entradas. Desse modo, tem-se uma noção satisfatória acerca da

segurança e qualidade do cifrador e, com isso, o dispositivo pode finalmente ser materializado e fabricado.

2 - Metodologia

Os polinômios de Fibonacci foram estudados (ou definidos) pela primeira vez em 1883, pelo matemático belga Eugene Charles Catalan (1814 – 1894) e pelo matemático alemão Ernest Erich Jacobsthal (1881 – 1965). Catalan introduziu a família de funções polinomiais de Fibonacci através da seguinte definição.

Definição 1: Chamaremos de Sequência Polinomial de Fibonacci – SPF, ao conjunto de funções polinomiaisdescritospelarelaçãoderecorrência f1(x) = 1,f2(x)= x, fn(x) x.fn-1(x) + fn-2(x), para n > 1.Ou de modo equivalente fn+1(x) = xfn(x)+fn-1(x).

São muito úteis para circuitos em si, podendo ser mapeados. Nesses casos foram mapeados para serem fontes geradoras de números pseudo-aleatórios utilizando o LSFR. Esses números podem posteriormente ser utilizados para criptografar algum tipo de informação, como uma imagem, por exemplo.

Após utilizado algum tipo de polinômio de fibonacci em um LSFR, obtêm-se uma sequência de números binários. Observe o exemplo abaixo:

Polinômio: $x^4 + x^3 + 1$

```
1111
1110
1100
1000
0001
0010
0100
1001
0011
0110
1101
1010
0101
1011
0111
1111
1110
1100
1000
0001
0010
0100
1001
0011
0110
1101
1010
0101
1011
0111
1111
```

É interessante notar que, após a exibição de todos os 15 estados, a sequência se repete.

Para sua execução, utilizou-se um código em verilog com uma bancada de testes para se obter os resultados. Um exemplo de código segue abaixo:

SV/Verilog Testbench

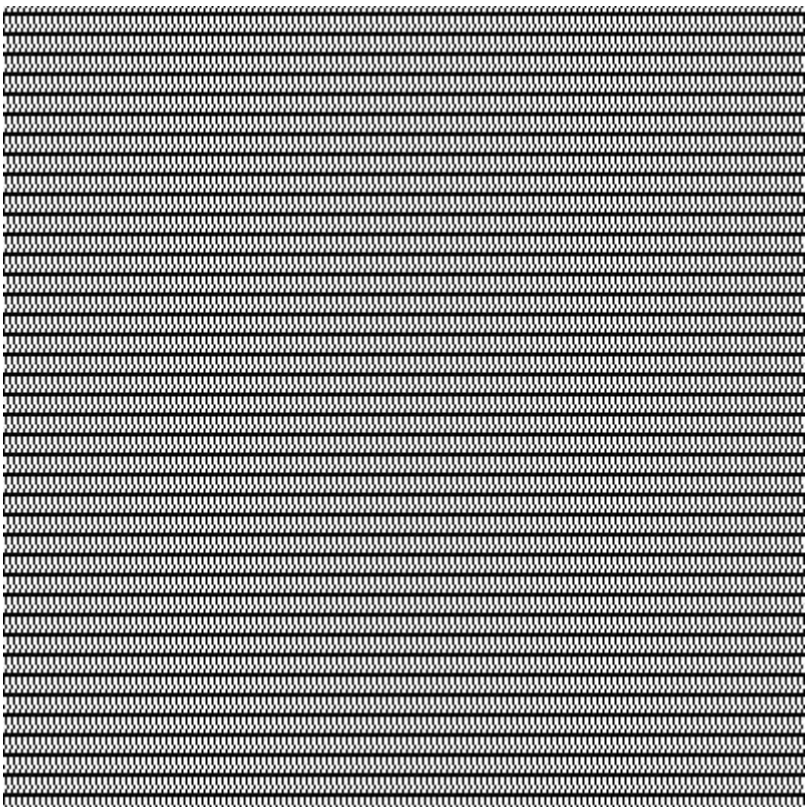
```
// Code your testbench here
// or browse Examples
module LFSR4_test;
  reg clock;
  wire [3:0] out;
  integer file;

  LFSR4 lfsr(clock, out);

  initial begin
    file = $fopen("output.txt", "w");
    if (file == 0) $display("Error opening the file!");
  end

  initial begin
    clock = 1'b0;
  end

  always #1 clock = ~clock;

  reg lastBit;
  initial begin
    repeat (160000) begin
      lastBit <= out[0];
      $fdisplay(file, "%b", lastBit);
      #1;
    end
  $fclose(file);
  #160000 $finish;
  end
endmodule
```

```
// Code your design here
module LFSR4 (
  input clk,
  output reg[3:0] LFSR = 15
);

  wire feedback = LFSR[3];

  always @(posedge clk)
    begin
      LFSR[1] <= LFSR[0];
      LFSR[2] <= LFSR[1];
      LFSR[3] <= LFSR[2];
      LFSR[0] <= (LFSR[2] ^ feedback);
    end

endmodule
```

3 - Resultados Obtidos

Depois de gerados os números binários, utiliza-se uma imagem totalmente branca a fim de criar a chave. Após isso, mistura-se a imagem branca com os bits mais significativos dos números binários gerados pelo LFSR, modificando, assim, os pixels da imagem branca.

Chave:

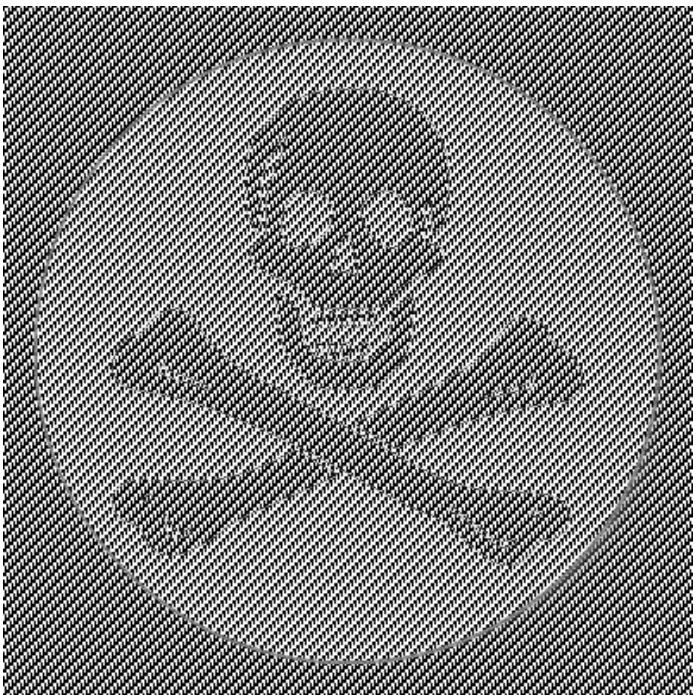


Com a chave, é possível pegar algum tipo de informação e torná-la irreconhecível a partir das práticas mencionadas neste documento. A imagem abaixo gera um resultado satisfatório.

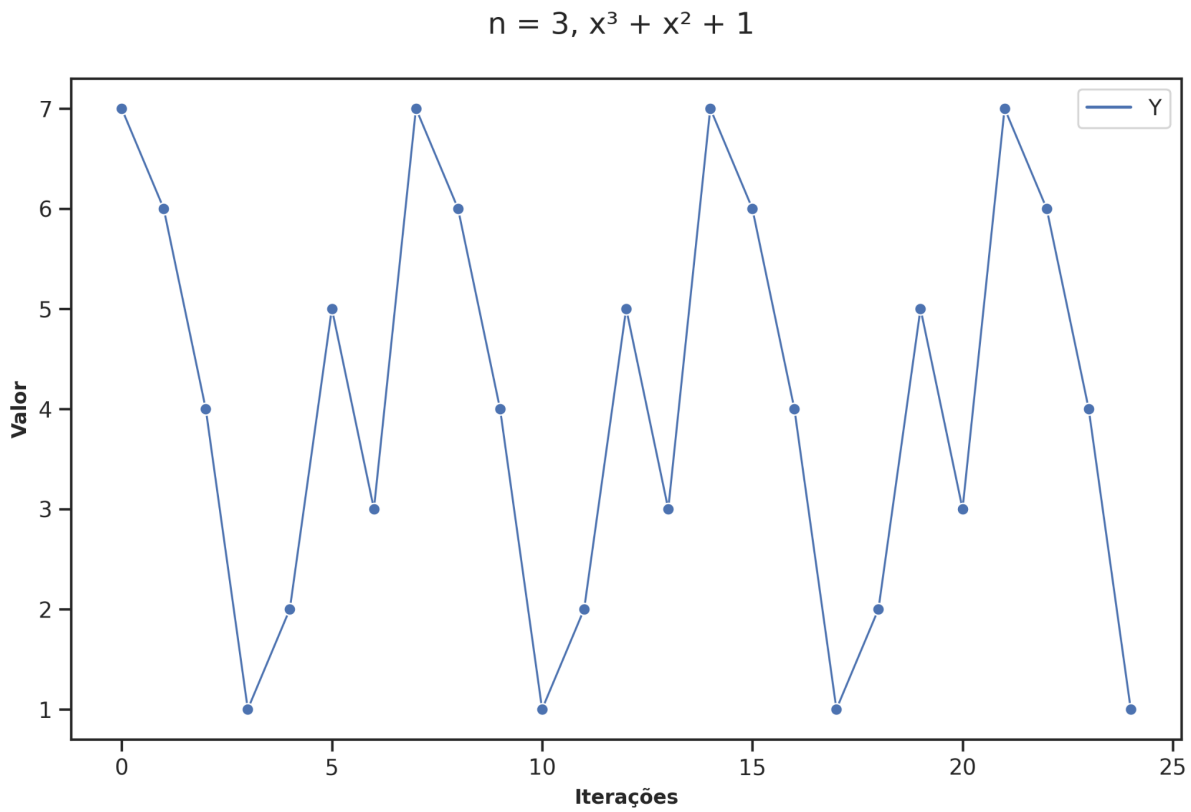
Imagem padrão:

Quando une-se a imagem à chave em questão, temos o seguinte resultado:

Imagem criptografada

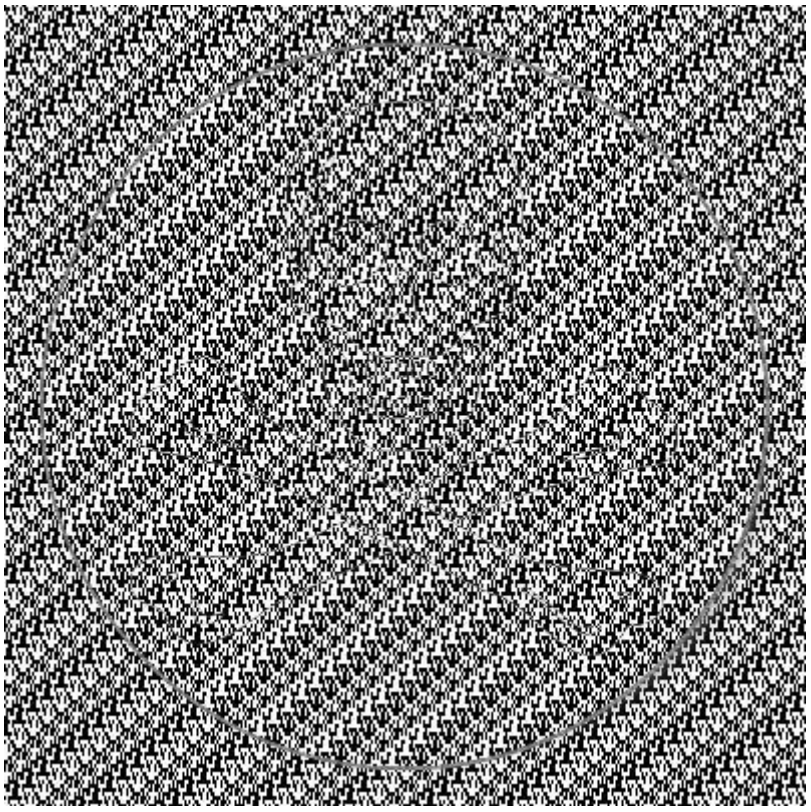


Note que, mesmo mesclada com a chave, ainda é possível reconhecer levemente a imagem original. Isso se dá ao fato de que a chave gerada e demonstrada anteriormente é provida de um polinômio de grau 3, o que gera ciclos muito baixos para números aleatórios. O gráfico abaixo mostra os ciclos gerados por esse polinômio.



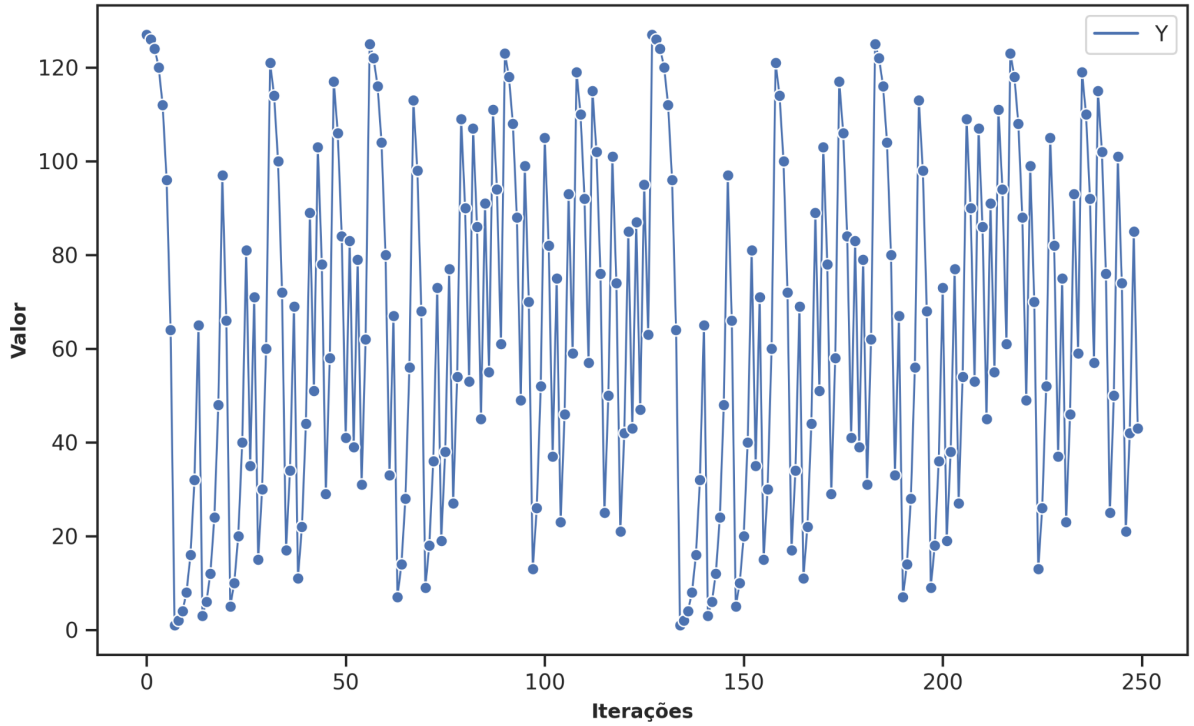
A mesma imagem, quando submetida a uma chave gerada pelo mesmo método porém utilizando um polinômio de grau 7, exibe o seguinte resultado de mesclagem:

Imagem criptografada



Aqui temos um resultado mais satisfatório, pois a imagem está praticamente irreconhecível. Pode-se tirar como conclusão que, a partir desse grau, tem-se cada vez mais segurança na informação passada. Isso se deve ao fato de que, para esse grau, temos um maior número de ciclos, como mostrado no gráfico abaixo.

$$n = 7,\ x^7 + x^6 + 1$$



O mesmo método permite que, ao fazer-se o inverso, obtenha-se a mesma mensagem original, basta utilizar-se uma nova porta XOR.

Imagem descriptografada

4- Conclusões

Após os estudos necessários para a execução do trabalho, foi possível concluir que, com o desenvolvimento de um mundo cada vez mais tecnológico, grandes preocupações surgem, sendo uma delas a segurança dos dados. Os métodos aqui demonstrados são fortes

exemplos de como esse assunto é relevante. Além disso, as aulas gravadas e o curso de introdução aos sistemas lógicos, ministrado pelo professor Gilberto Medeiros Ribeiro (UFMG), foram de grande auxílio para a execução deste projeto. O projeto não só possibilitou a prática de muitos conteúdos aprendidos em sala, mas também enriqueceu os conhecimentos dos alunos com novos conteúdos do campo de hardware.

5 - Referências

Donda, Daniel. One-Time pad, a criptografia inquebrável. Disponível em: https://danieldonda.com/one-time-pad-otp-a-criptografia-inquebravel/. Acesso em 20 de junho de 2023.

Linear Feedback Shift Register. Disponível em: https://www.sciencedirect.com/topics/mathematics/linear-feedback-shift-register. Acesso em 20 de junho de 2023.

Medeiros, Gilberto. Aulas gravadas. Disponível em: https://www.youtube.com/@gilbertomedeirosribeiro6785/featured. Acesso em 20 de junho de 2023.