Avaliando a Aleatoriedade do Gerador de Números Aleatórios em um *Smart Card* Comercial

Acadêmicos:
Heloiza Paulichen
Leonardo Cícero Marciano
Vinicius Tartari

Câmpus Pato Branco
UTFPR
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CÂMPUS PATO BRANCO
MINISTÉRIO DA EDUCAÇÃO
BRASIL
GOVERNO FEDERAL

Definições

- O que é um *Smart Card?*
- Gerador de Números Aleatórios (RNG)
  - Pseudo RNG
  - True RNG

Introdução

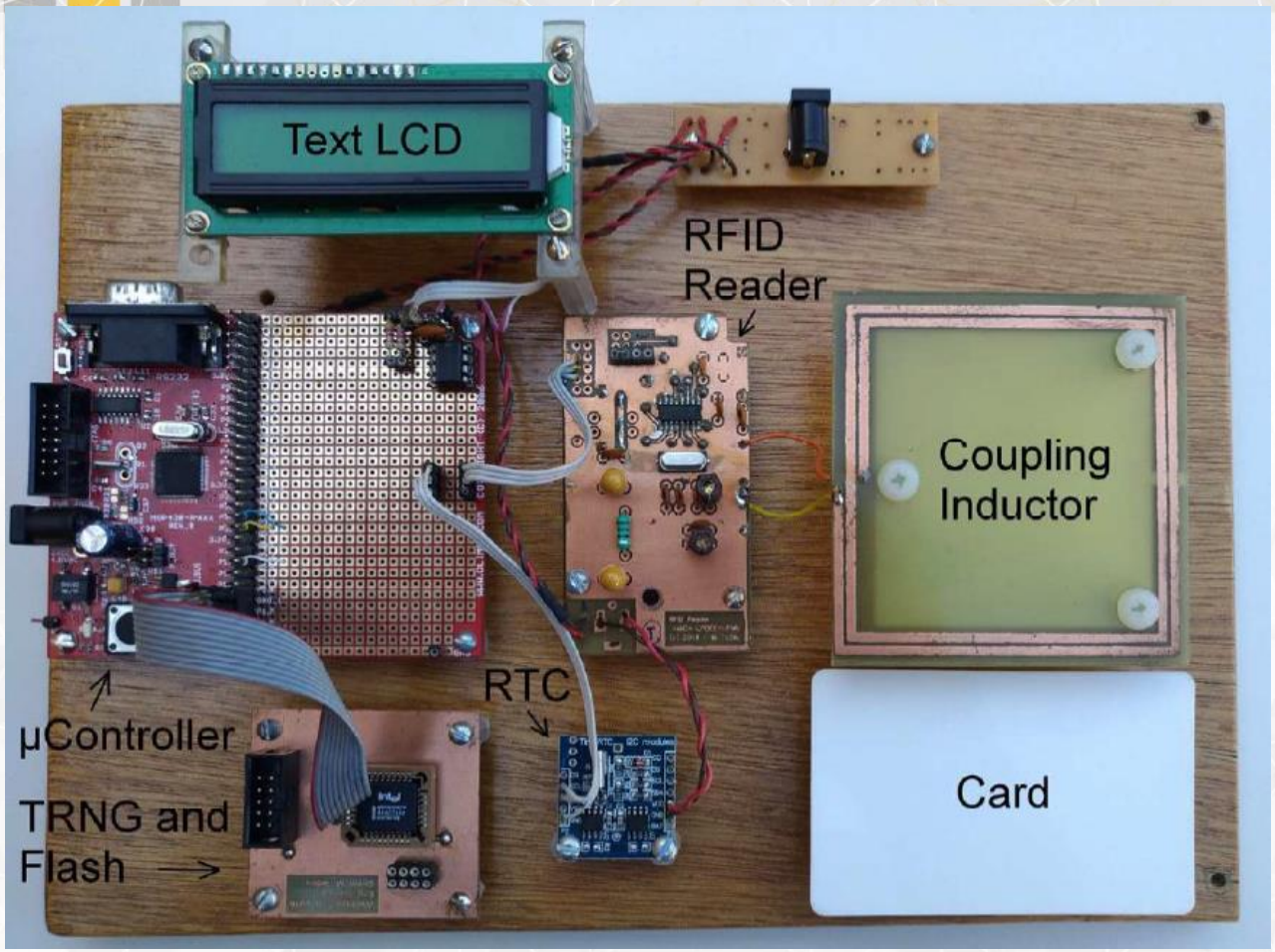
- Ataques a esse tipo de *hardware* podem ocorrer sem nenhum tipo de restrição.
- Vulnerabilidade devido as limitações dos *Smart Cards*.
- Estudos recentes indicam falhas de segurança, uma parte pela fraca aleatoriedade do PRNG.
- Comparação entre PRNG e TRNG.

Qualificando um RNG

- Métodos estatísticos
- Até mesmo os melhores RNGs podem falhar
- *Statistical Test Suite* (STS) da *National Institude of Standards and Technolgy* (NIST)

Aquisição de Dados

- Utilizados três *Smart Cards* idênticos
- Interface sem contato, RFID na norma ISO 14443B
- Controle de entrada
- Taxa máxima de 150 bps para obtenção de dados
- Desenvolvido um leitor de RFID para o trabalho
  - Envolve microcontrolador, tela LCD alfanumérica, RTC, comunicação com PC, memória flash e o Intel i82802 para o TRNG.


Text LCD
RFID
Reader
Coupling
Inductor
RTC
µController
TRNG and
Flash
Card

TRNG: Intel i82802

- É um IC com *Firmware* para *Chipsets* Intel
- Entre várias características, contém um TRNG
- Utiliza ruído térmico proveniente das propriedades do silício presente no *chip*
- Principal desvantagem: alto consumo de energia
  - Chip permanece funcional independente do sistema necessitar de números aleatórios ou não

Metodologia

- Adquirido uma grande quantidade de *bits*, armazenados em arquivos no PC que controlava a aquisição.
- Aquisição em dois modos
  - On-Off
  - Contínuo

Metodologia

- Processado pelo STS em blocos de n *bits*
  - É ideal que n seja igual ou maior que 10^5
- Qualificação por meio de aquisição de m sequências de n *bits*
- 96% de aprovação qualifica o gerador como satisfatório
- No estudo, m = 10^2 e n = 10^5
- A aquisição desses dados levou 18 horas no modo contínuo e 7 dias em on-off. No TRNG levou 59 minutos, e somente o modo contínuo foi testado.

Os Testes

- **Frequência (*Monobit*):** Verifica a proporção de 0s e 1s na sequência inteira.
- **Frequência em Bloco:** Idem anterior, porém em blocos de M bits.
- **Somas Cumulativas:** Soma os bits da sequência e determina a excursão máxima.
- ***Run*:** Encontra o número de runs. *Run* é uma sequência ininterrupta de bits idênticos.
- ***Run* mais Extenso:** Encontra o maior *run* de 1s em um bloco de M bits.

Os Testes

- **Posto de Matriz Binária:** Calcula o posto de submatrizes disjuntas da sequência. Procura dependências lineares em *substrings* da sequência original.
- **FFT:** Aplica a transformada de Fourier na sequência para encontrar padrões repetitivos e próximos.
- **Modelo Sobreposto:** Procura o número de ocorrências de uma *substring* específica de m *bits*.
- **Entropia Aproximada:** Determinar a frequência de todos os padrões sobrepostos de m *bits* sobre toda a sequência. Compara a frequência com a de um bloco de m+1 *bits* e o resultado esperado de uma sequência aleatória.

Os Testes

- **Excursões Aleatórias:** Procura o número de ciclos contendo K visitas em uma soma cumulativa.
- **Variante de Excursões Aleatórias:** Procura o número de vezes que determinado estado foi visitado em uma soma cumulativa.
- **Serial:** Idem Modelo Sobreposto, porém o tamanho da sequência a ser testada é de 2^m bits.
- **Complexidade Linear:** Testa se a sequência é complexa o suficiente para ser aleatória utilizando LFSR (*Linear Feedback Shift Registers*).

Os Testes

- **Universal:** Se refere ao Teste Estatístico Universal de Maurer. Consiste em encontrar o número de *bits* entre dois padrões, com o intuito de detectar se a sequência pode ser comprimida sem perca de informação.

Os Testes

- **Modelo Não-Sobreposto:** Assim como o modelo sobreposto, procura o número de ocorrências de uma *substring* de m *bits*. O que o diferencia do Sobreposto é o que ocorre quando uma sequência igual a *substring* é encontrada. Aqui, a janela de procura avança para o bit depois do fim da sequência. No sobreposto, ela avança somente um *bit*.

Resultados

Taxa de aprovação das sequências do STS-NIST em porcentagem, modo contínuo.

Teste	i82802	Cartão 1	Cartão 2	Cartão 3
Frequência (Monobit)	99	93	81	73
Frequência em Bloco	100	100	94	62
Somas Cumulativas (Avançando)	98	90	81	74
Somas Cumulativas (Retrocedendo)	99	94	81	73
Run	99	94	75	88
Run Mais Extenso	100	71	80	20
Posto de Matriz Binária	100	99	99	29
FFT	100	100	70	0
Modelo Sobreposto	99	98	97	39
Entropia Aproximada	100	6	12	0
Excursões Aleatórias	100	100	100	100
Variante de Excursões Aleatórias	100	100	100	100
Serial	98	94	68	0
Complexidade Linear	97	97	99	87
Universal	100	90	70	60

Resultados

Taxa de aprovação das sequências do STS-NIST em porcentagem, modo on-off.

Teste	Cartão 1	Cartão 2	Cartão 3
Frequência (Monobit)	15	21	12
Frequência em Bloco	24	33	36
Somas Cumulativas (Avançando)	2	14	6
Somas Cumulativas (Retrocedendo)	4	15	6
Run	5	7	4
Run Mais Extenso	32	32	22
Posto de Matriz Binária	85	88	75
FFT	0	0	0
Modelo Sobreposto	42	58	34
Entropia Aproximada	11	10	14
Excursões Aleatórias	NE	NE	NE
Variante de Excursões Aleatórias	NE	NE	NE
Serial	82	85	68
Complexidade Linear	99	100	99
Universal	0	0	1

Resultados

Taxa de aprovação das sequências do STS-NIST em porcentagem, modo contínuo, teste de Modelo Não-Sobreposto.

	i82802	Cartão 1	Cartão 2	Cartão 3
Número de modelos em que o teste falhou	1	43	23	148
Maior porcentagem de reprovação	5%	20%	13%	72%

- Para este teste, foi utilizado o teste do modelo não-sobreposto com 148 padrões diferentes.
- Considerando cada padrão diferente como um teste separado, foram executados 163 testes no total.

Resultados

- O TRNG teve um comportamento adequado, sendo aprovado em todos os testes.
- O *Smart Card* 2 obteve melhor resultado, apesar de uma taxa de reprovação alta em alguns testes.
- Para os resultados vistos no modo on-off, é possível examinar de forma indireta o aspecto da semente que inicia o gerador.
- Devido a alta aprovação no teste de complexidade linear, que permite inferir que o gerador nestes cartões são baseados em LFSR.

Conclusão

- Não é possível dizer que o RNG analisado é de fato utilizado na unidade criptográfica do *Smart Card*. Porém, seja isso o caso, expõe-se uma grave falha de segurança sobre este hardware.
- É possível que um dos *Smart Cards* seja defeituoso devido ao resultado tão aquém do esperado. Se a proporção de cartões defeituosos é significativa, isto também gera uma preocupação em relação a segurança.