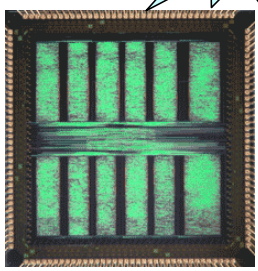
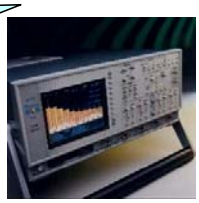
A power disturbance circuit for A5/1 resistant to power analysis attack

修士課程修了　戴　偉

Background

Great Crisis



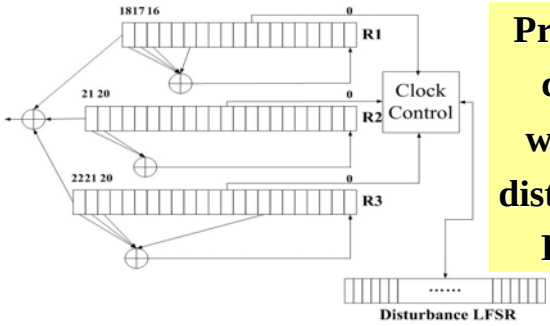


Power wiretap and analysis

Various waveform characteristics (Peak, Shape, etc)

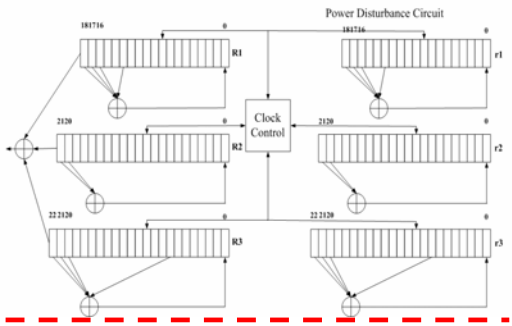
Systemic and valuable validation parameters are required!

Proposed power disturbance circuits



Proposed circuit with one disturbance LFSR

Proposed circuit with three disturbance LFSRs



Proposed validation parameters

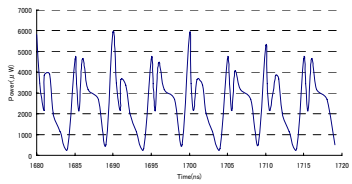
$$D_{(AP)} = \frac{\sum_{n=0}^{1000}[Power_{(3LFSR)}(n) - Power_{(2LFSR)}(n)]}{\sum_{n=0}^{1000} Power_{(3LFSR)}(n)} \times 100\%$$

$$D_{(PP)} = \frac{\sum_{n=0}^{1000}[Peak_{(3LFSR)}(n) - Peak_{(2LFSR)}(n)]}{\sum_{n=0}^{1000} Peak_{(3LFSR)}(n)} \times 100\%$$

$$P_{x,y} = \frac{Cov(x,y)}{\partial_x . \partial_y} \times 100\%$$

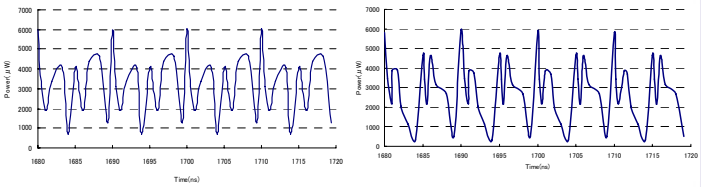
$$\mathrm{Cov(x,y)} = \frac{1}{n}\sum_{i-1}^{n}(x_i - \mu_x)(y_i - \mu_y)$$

Analysis and Conclusion

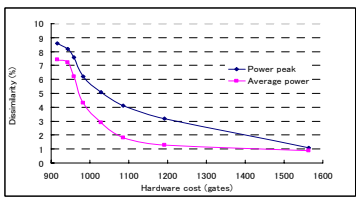


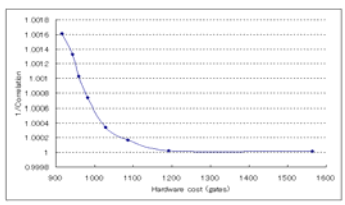
Vulnerable circuit

Better performance



Higher security





早稲田大学 大学院 情報生産システム研究科
システムLSI分野システムLSI応用部門　池永研究室