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

**Background**

- Various waveform characteristics (Peak, Shape, etc)
- Systemic and valuable validation parameters are required!

**Proposed validation parameters**

\[
D_{(AP)} = \sum_{n=0}^{1000} \left[ \text{Power}_{(3LFSR)}(n) - \text{Power}_{(2LFSR)}(n) \right] \times 100% / \sum_{n=0}^{1000} \text{Power}_{(3LFSR)}(n)
\]

\[
D_{(PP)} = \sum_{n=0}^{1000} \left[ \text{Peak}_{(3LFSR)}(n) - \text{Peak}_{(2LFSR)}(n) \right] \times 100% / \sum_{n=0}^{1000} \text{Peak}_{(3LFSR)}(n)
\]

\[
P_{x,y} = \frac{\text{Cov}(x, y)}{\sigma_x \sigma_y} \times 100%\]

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

**Proposed power disturbance circuits**

- Proposed circuit with one disturbance LFSR
- Proposed circuit with three disturbance LFSRs

**Analysis and Conclusion**

- Vulnerable circuit
- Better performance
- Higher security

- **Great Crisis**
- **Power wiretap**
- System LSIs