An Oscillator-Based True Random Number Generator with Process and Temperature Tolerance

Takehiko Amaki, Masanori Hashimoto and Takao Onoye

Osaka University
hasimoto@ist.osaka-u.ac.jp
Security and random number

- Cryptography and authentication system requires **unpredictable random numbers**. ex.) Private/Public key generation, challenge-and-response authentication, etc.

- Random number generator
  - Pseudo random number generator
    - Mathematical calculation
    - Output is **periodic and then predictable**.
  - True random number generator (TRNG)
    - Physical random source
    - Output is **unpredictable**.
Oscillator-based TRNG

- Acquires randomness from period jitters of oscs.
- **Pro:** Easy to implement
- **Con:** Difficult to generate highly random numbers
  - sensitive to duty cycle of fast osc.

![Diagram of Oscillator-based TRNG]

Duty cycle of fast osc. decides 0/1 probability.
Contribution

• Duty cycle variation due to temperature
  – Biases 0/1 probability beyond $50\pm0.125\%$ and makes TRNG fail in NIST randomness test.
  – Cannot be eliminated by static tuning at shipping test

• Developed a TRNG w/ dynamic 0/1 bias correction for process and temperature tolerance
  – Fast duty cycle monitor
  – Duty cycle adjuster
Dynamic duty cycle correction

- **Proposed duty cycle correction** sustained duty cycle and entropy under temperature variation between 0°C and 75°C.
  - Without it, duty cycle and entropy degraded.

![Graph 1](image1.png)

- Maximum error of probability of '1' [%]
- Minimum entropy
- Beyond 0.25%
- Entropy degradation
Comparison w/ existing works

- Among TRNGs that pass NIST tests, area of proposed TRNG is minimum.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Direct amp.</td>
<td>Osc.</td>
<td>Chaos</td>
<td>Metastable</td>
<td>Osc.</td>
</tr>
<tr>
<td>Tech.</td>
<td>180nm</td>
<td>90nm</td>
<td>180nm</td>
<td>45nm</td>
<td>65nm</td>
</tr>
<tr>
<td>Area (45nm)</td>
<td>1,563μm²</td>
<td>3,250μm²</td>
<td>7,875μm²</td>
<td>4,004μm²</td>
<td>3,335μm²</td>
</tr>
<tr>
<td>Randomness test</td>
<td>FIPS140-1 Knuth</td>
<td>AIS31 Entropy</td>
<td>NIST</td>
<td>NIST Entropy</td>
<td>NIST DIEHARD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Auto corr. Run length</td>
<td></td>
</tr>
</tbody>
</table>

1S-2