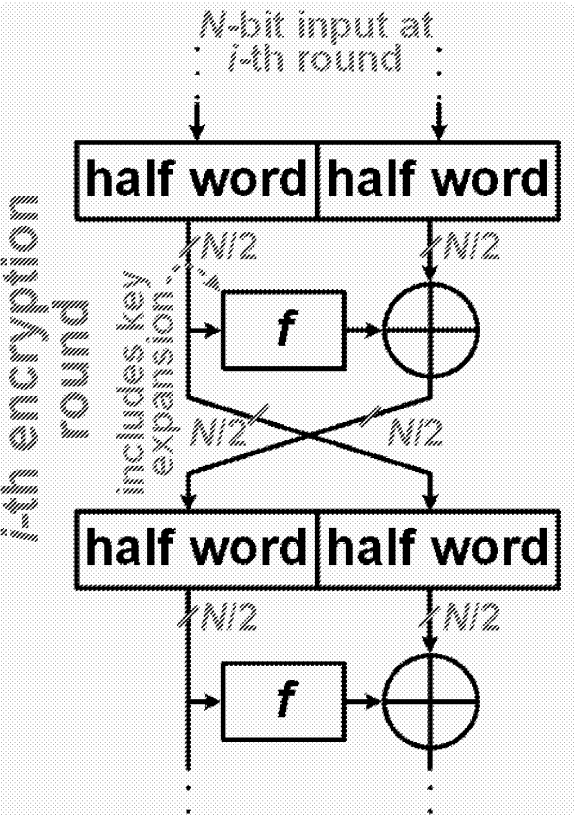
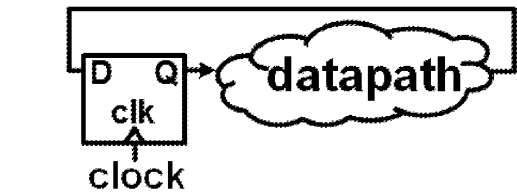


GENERAL FEISTEL NETWORK

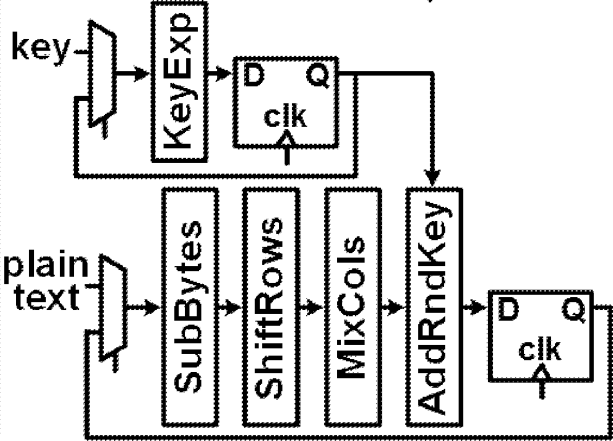


(a)

GENERALIZED STRUCTURE OF PRIVATE-KEY CRYPTO CORE (ITERATIVE ALGORITHMS)

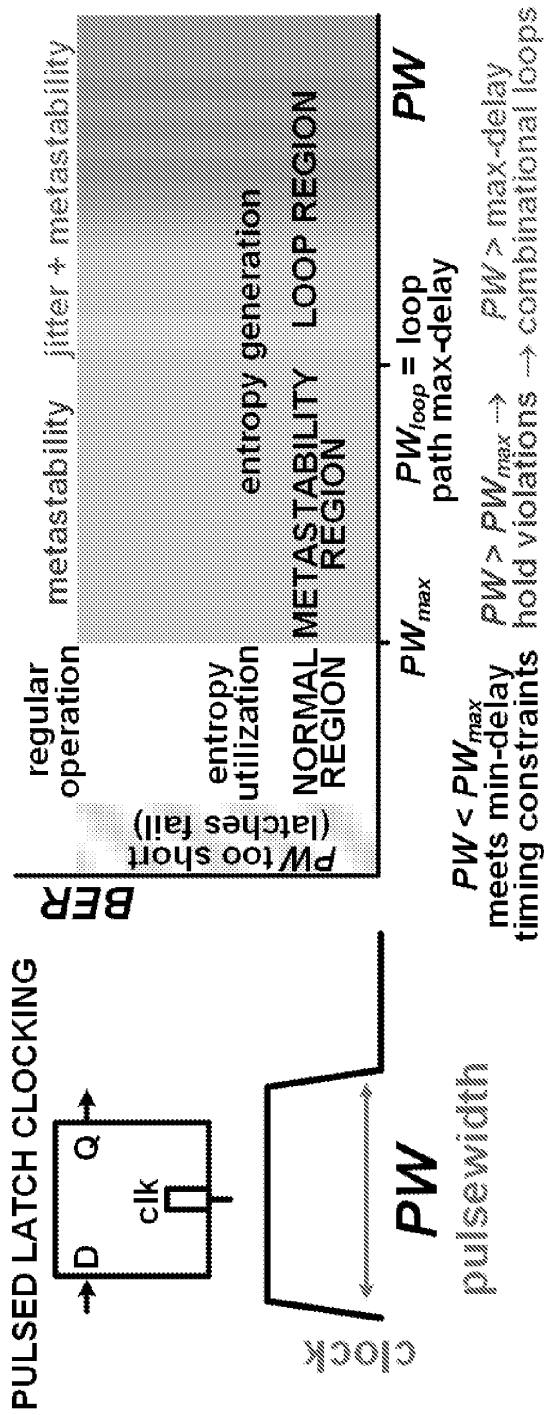


GENERALIZED SPN NETWORK (ADVANCED ENCRYPTION STANDARD)



(b)

Figure 1



(c)

Figure 1 (continued)

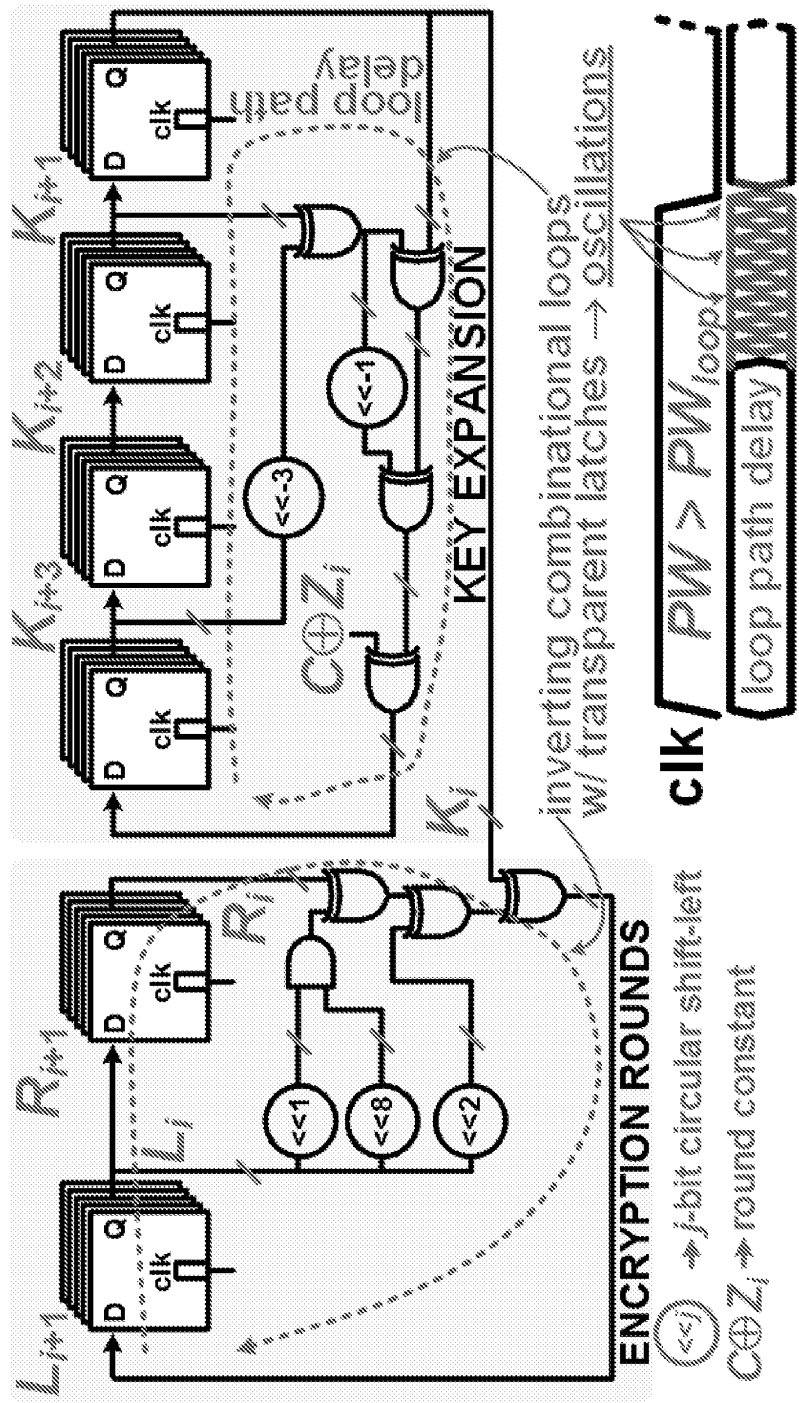


Figure 2(a)

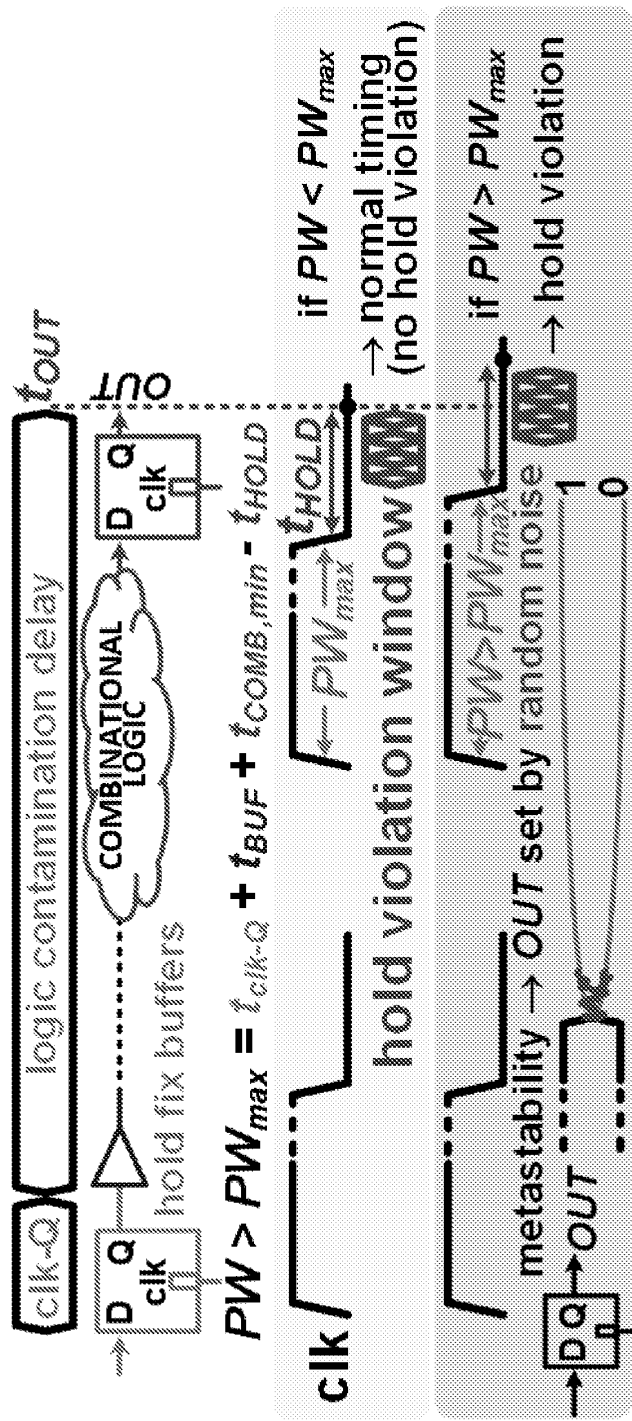


Figure 2(b)

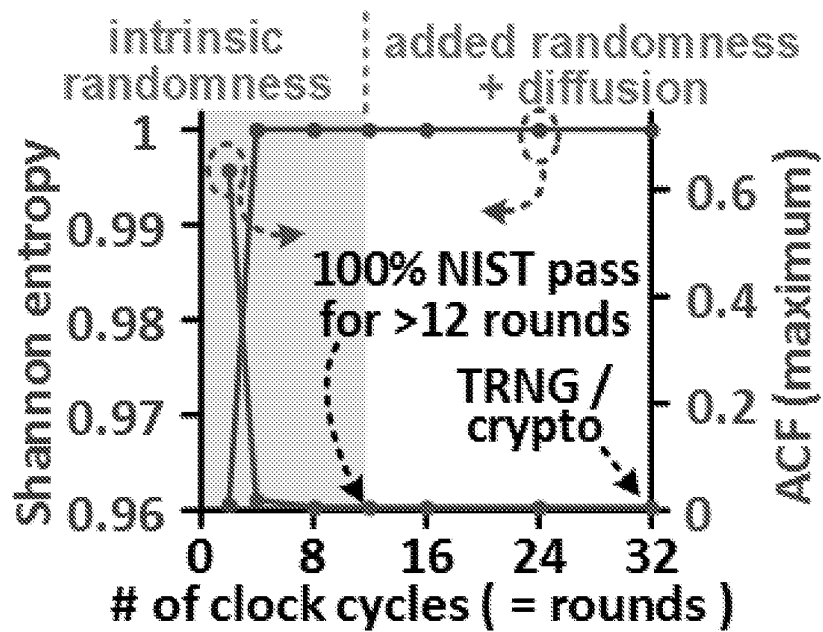


Figure 3(a)

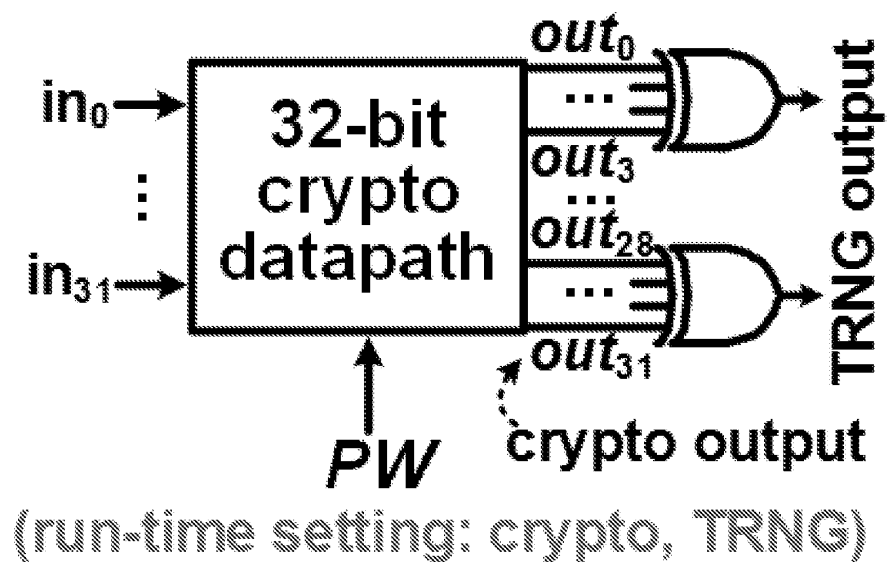


Figure 3(b)

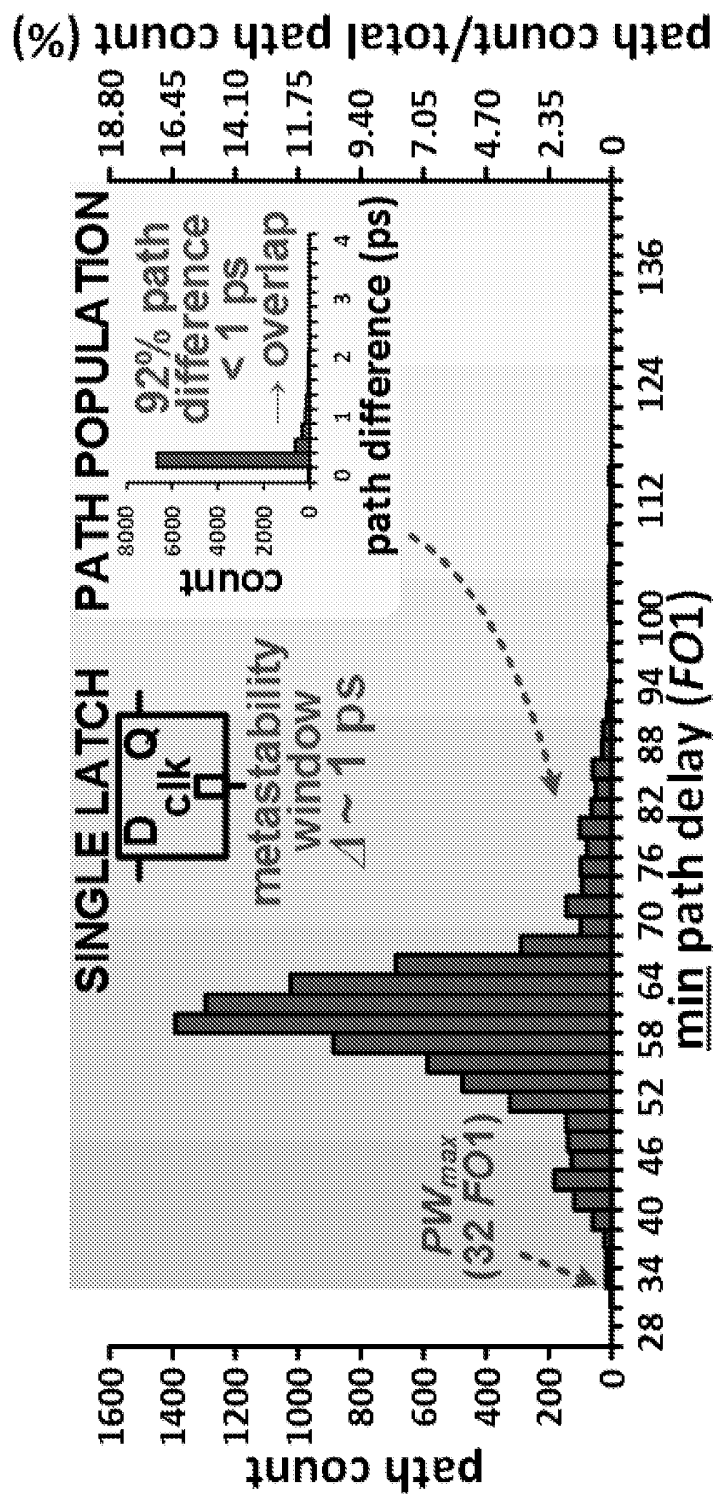


Figure 4

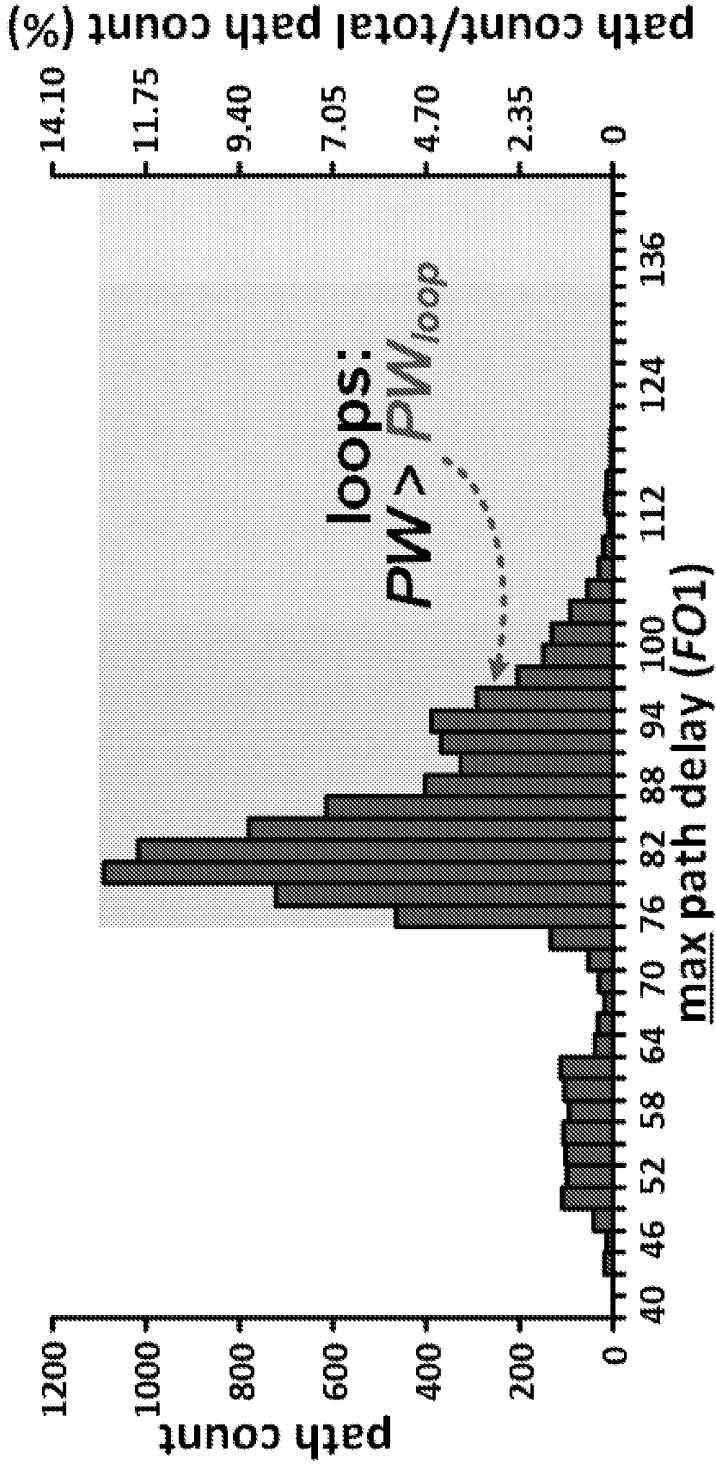


Figure 5

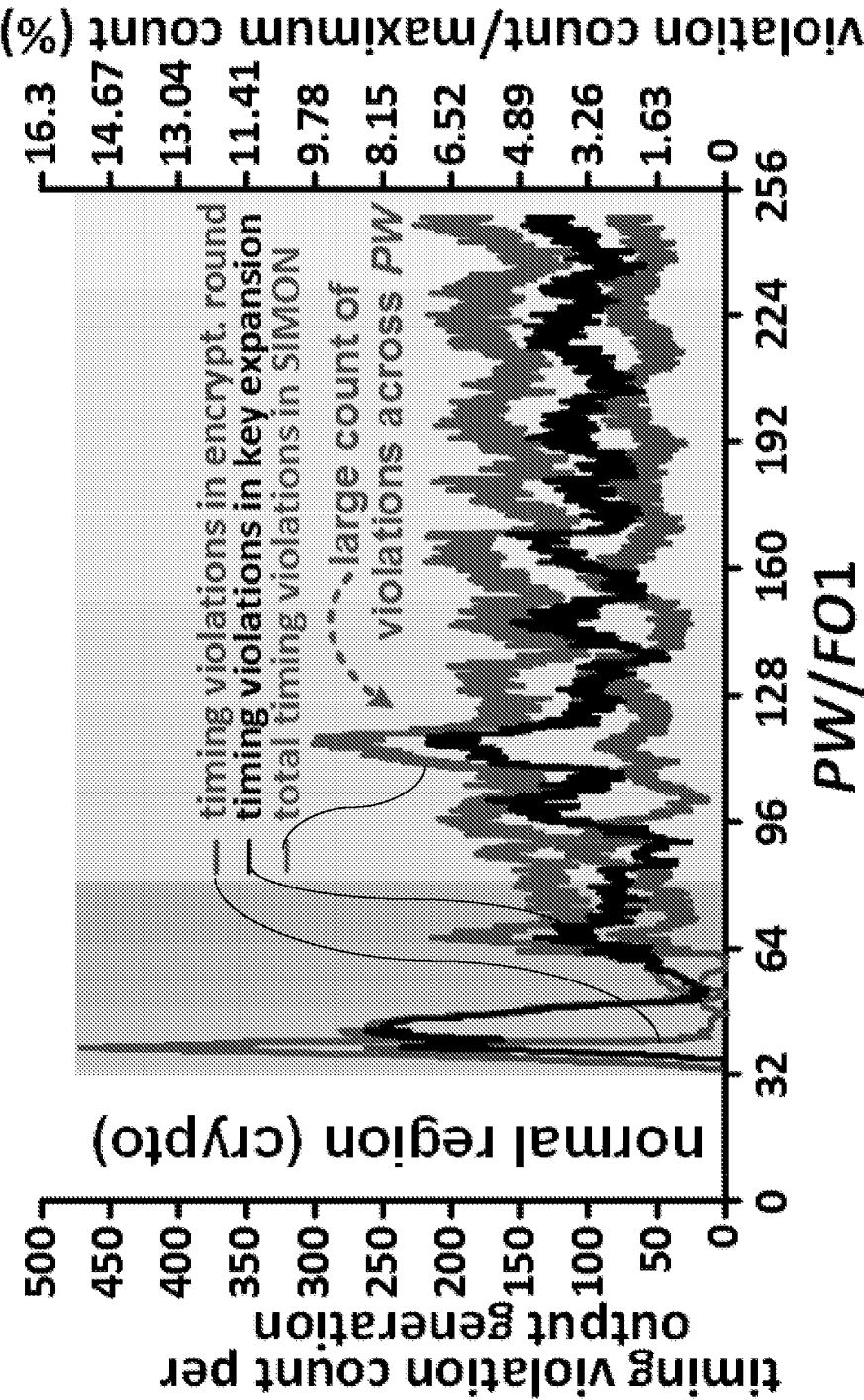


Figure 6(a)

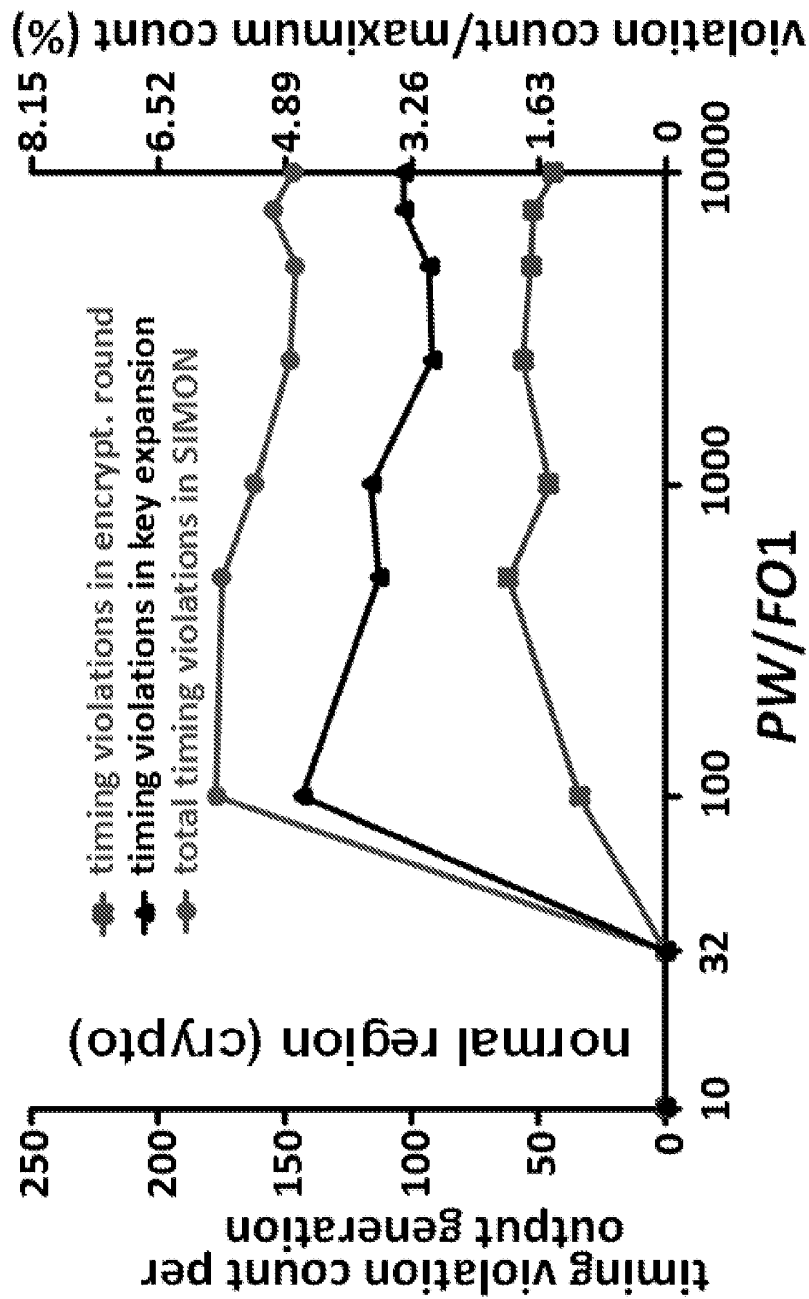


Figure 6(b)

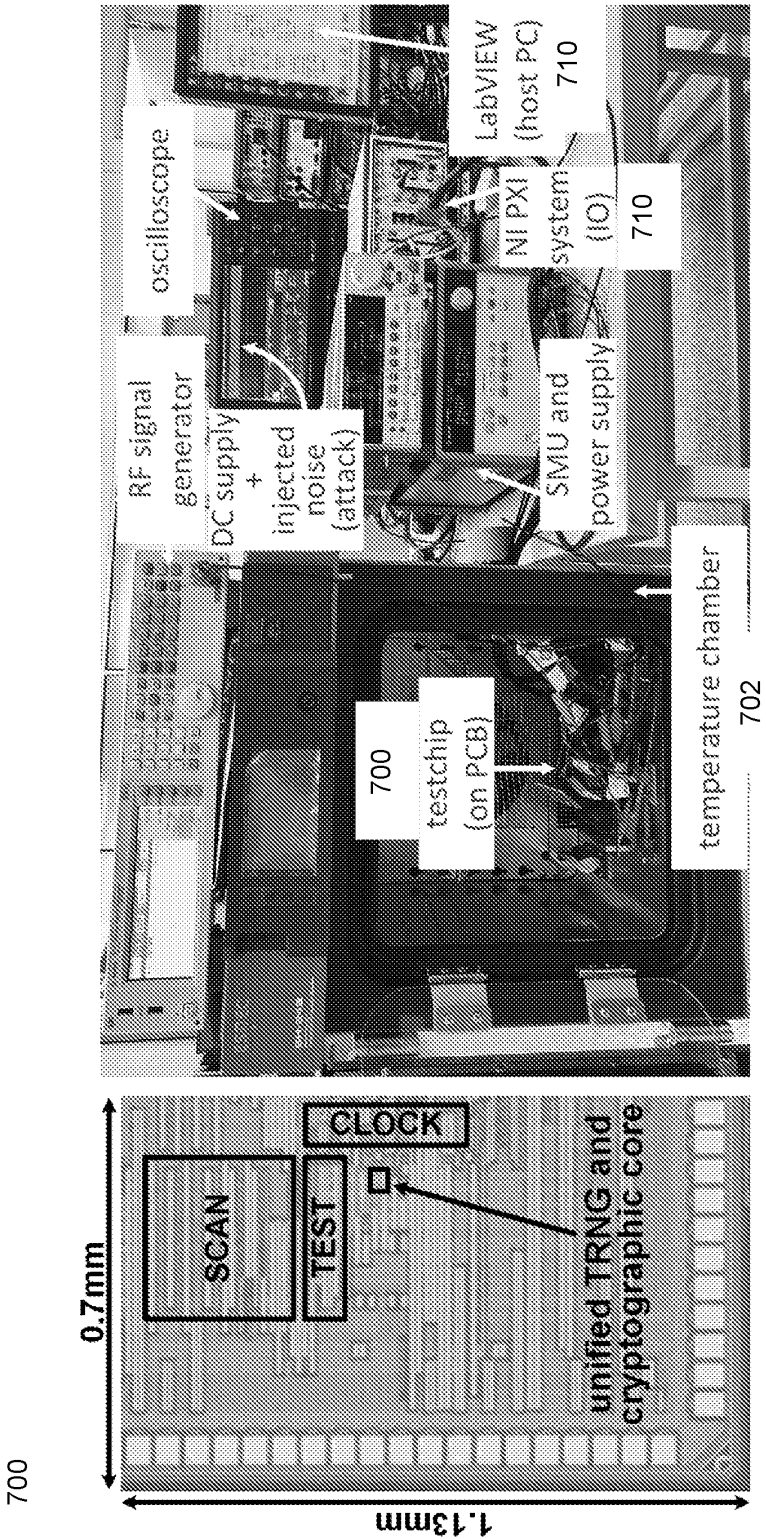


Figure 7(a)

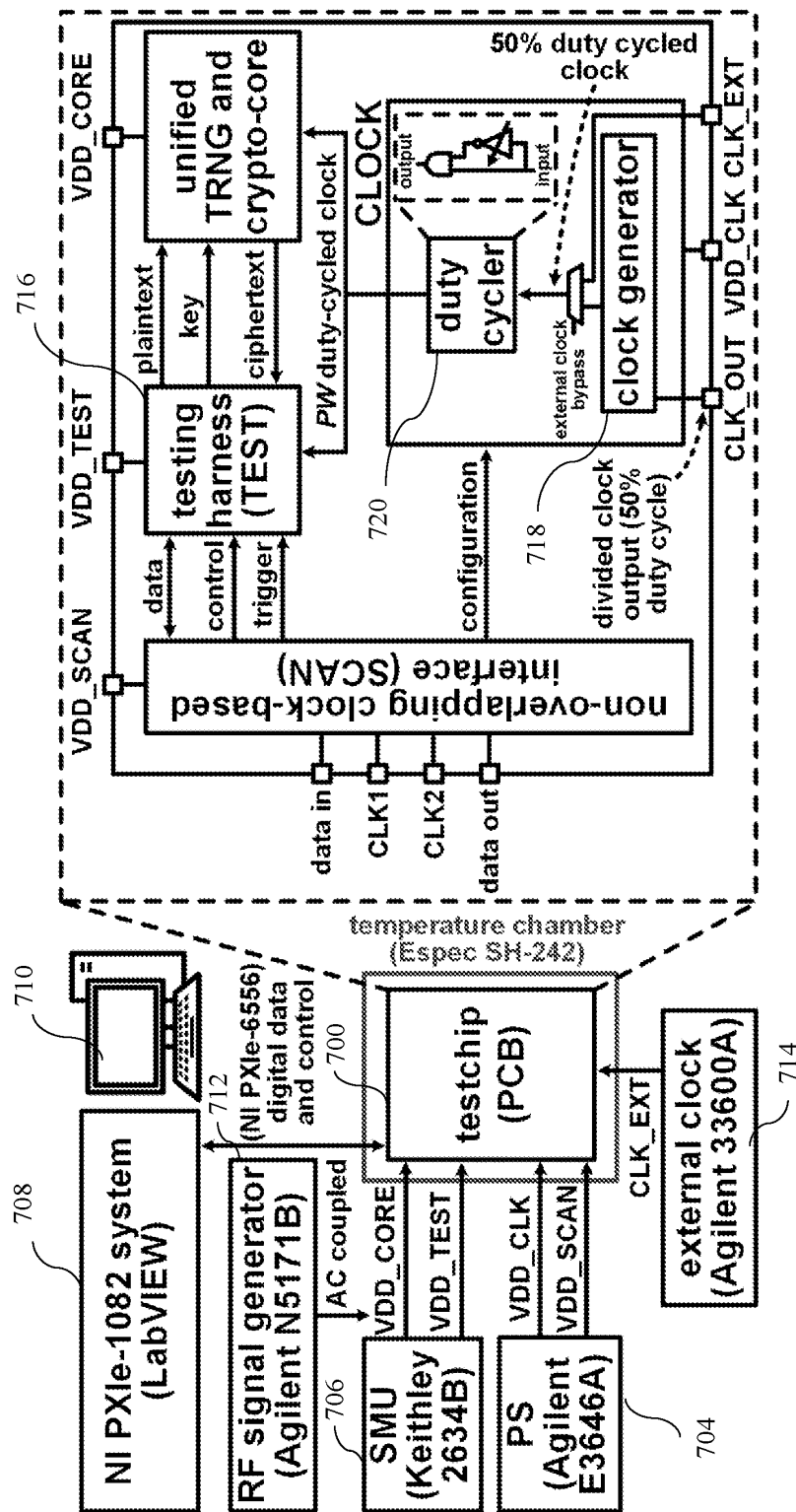


Figure 7(b)

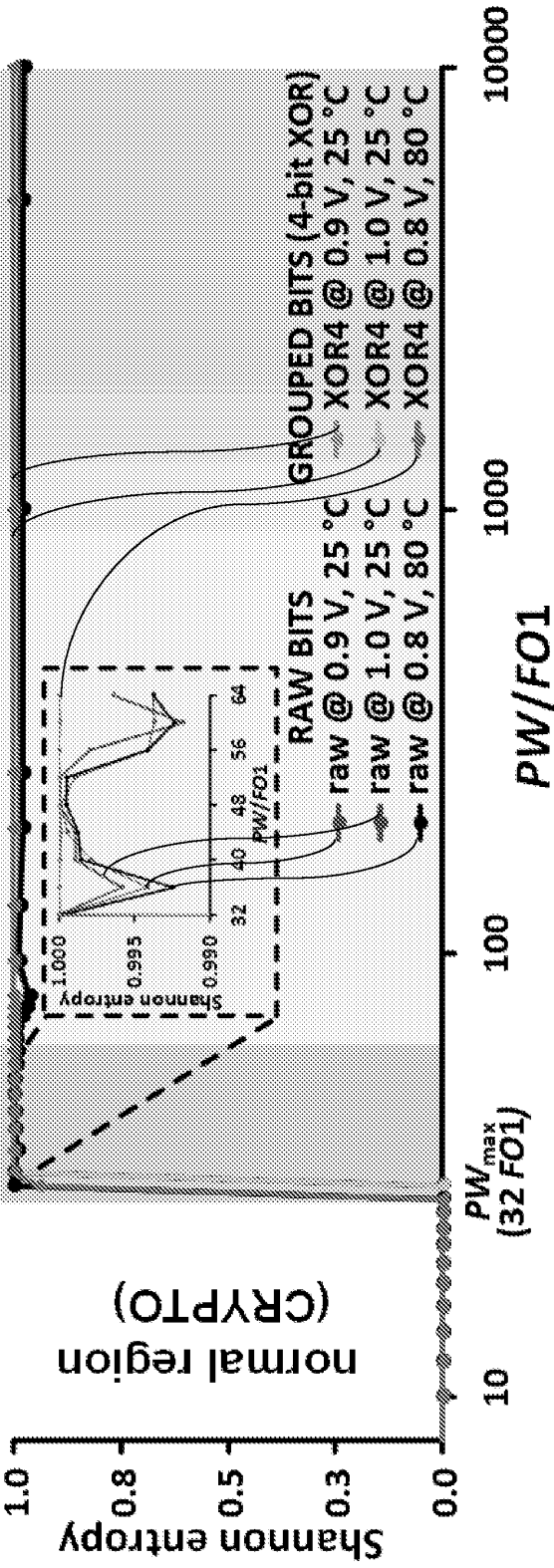
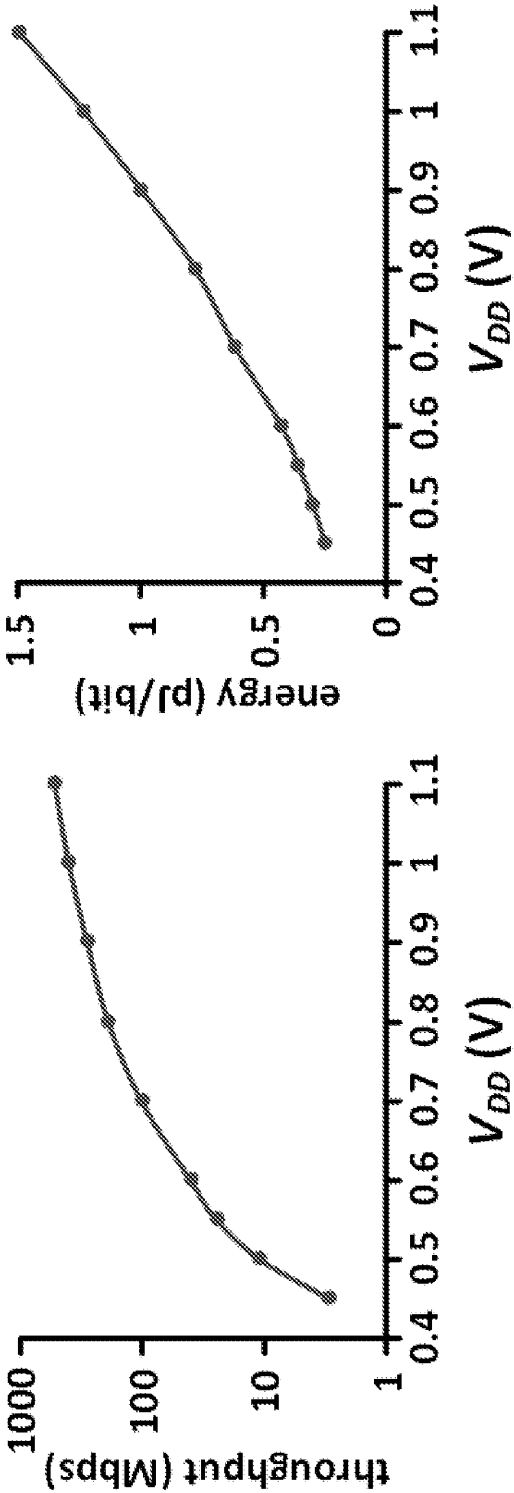


Figure 8



(b)

(a)

Figure 9

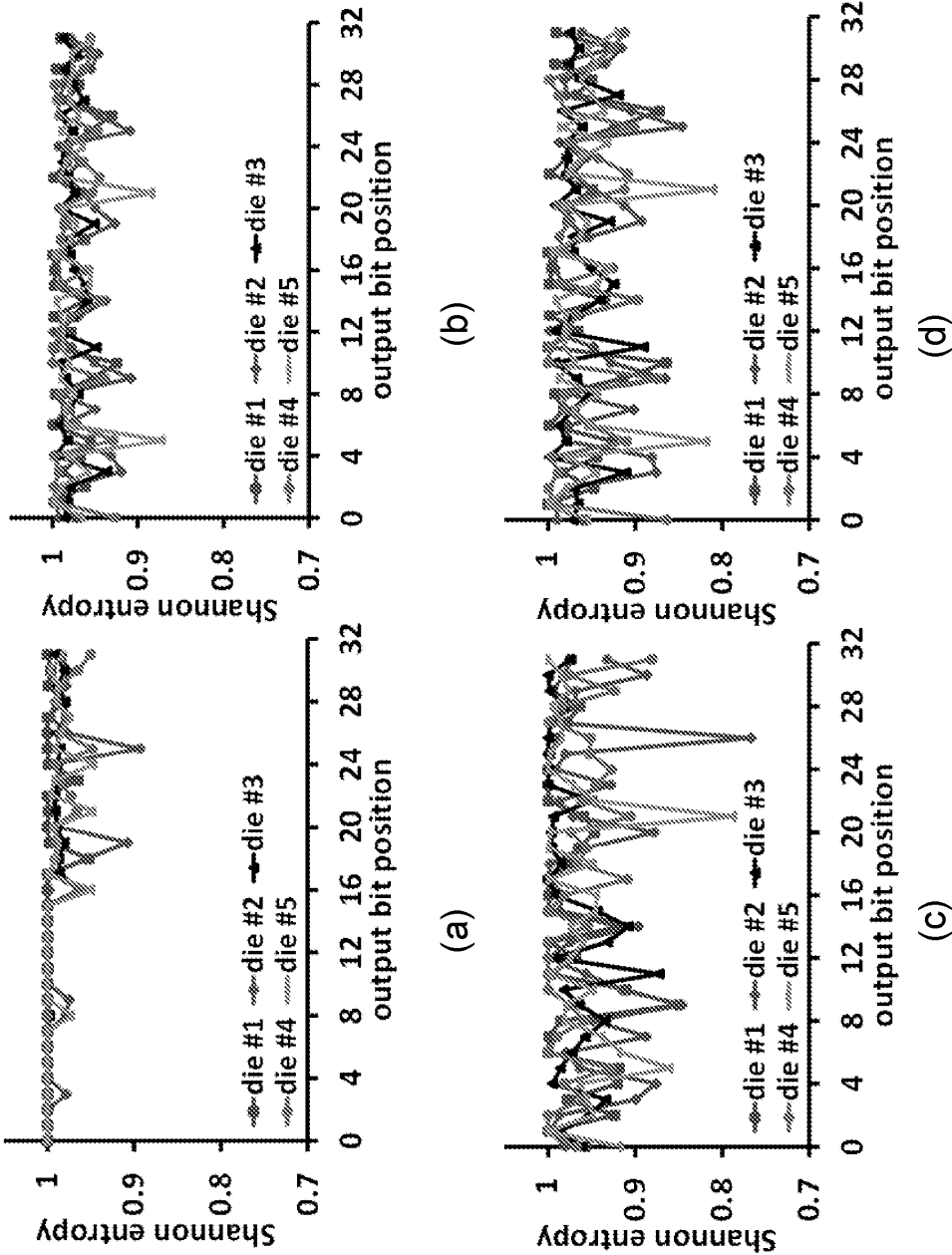


Figure 10

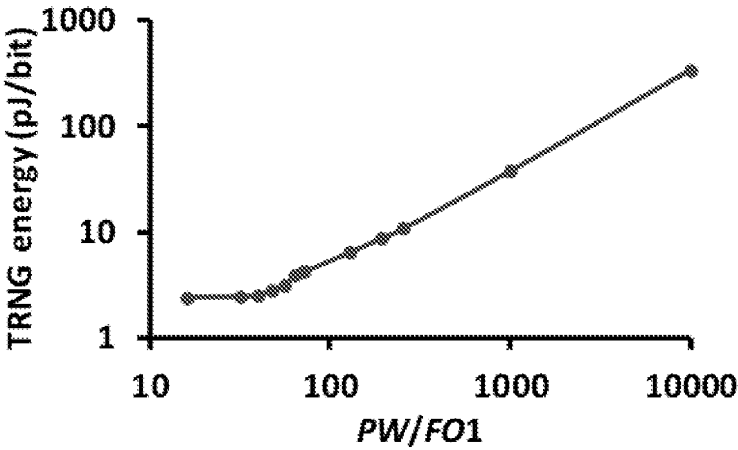


Figure 11

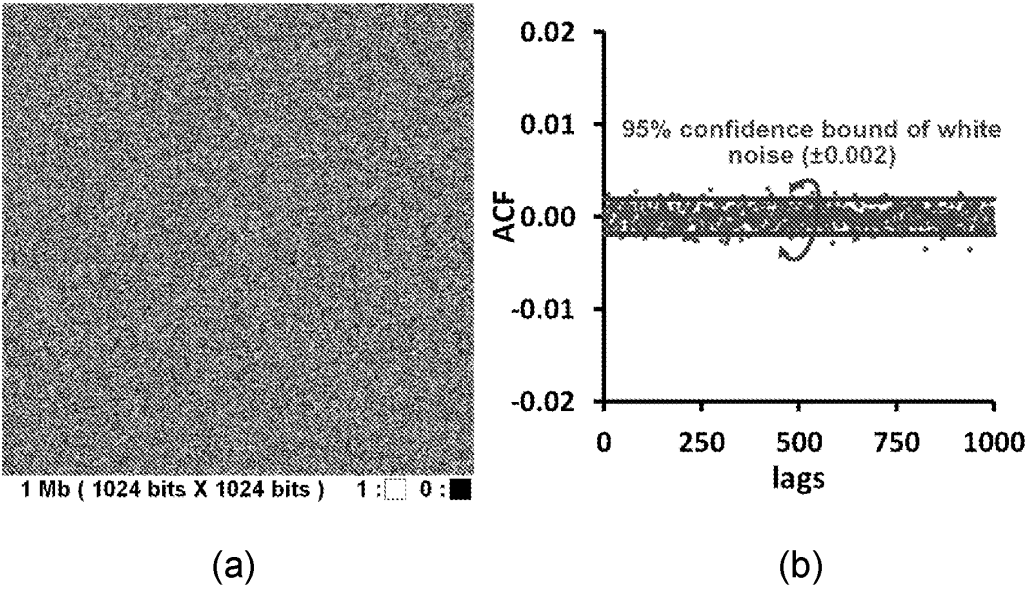


Figure 12

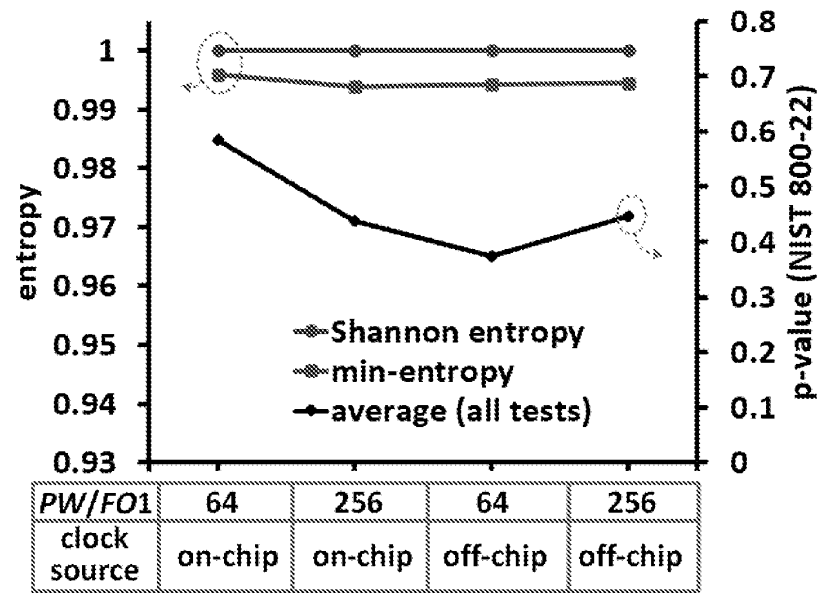


Figure 13

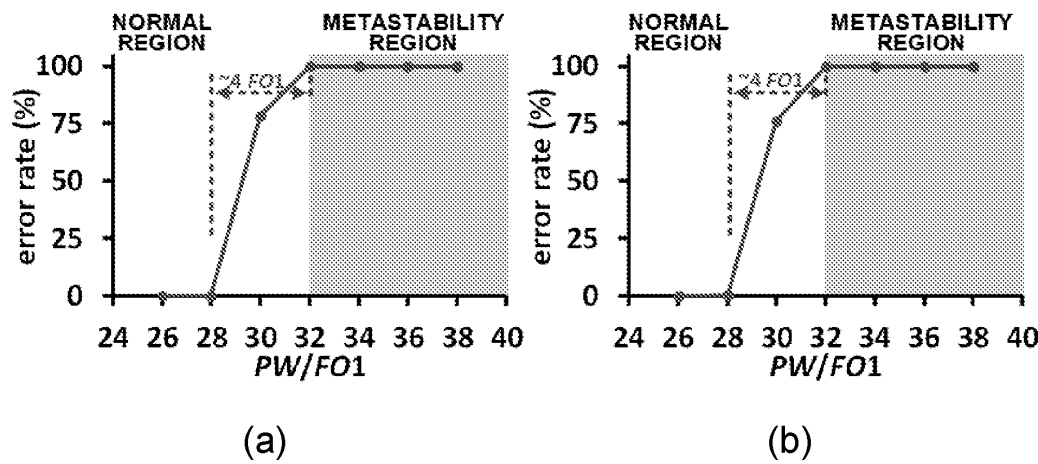


Figure 14

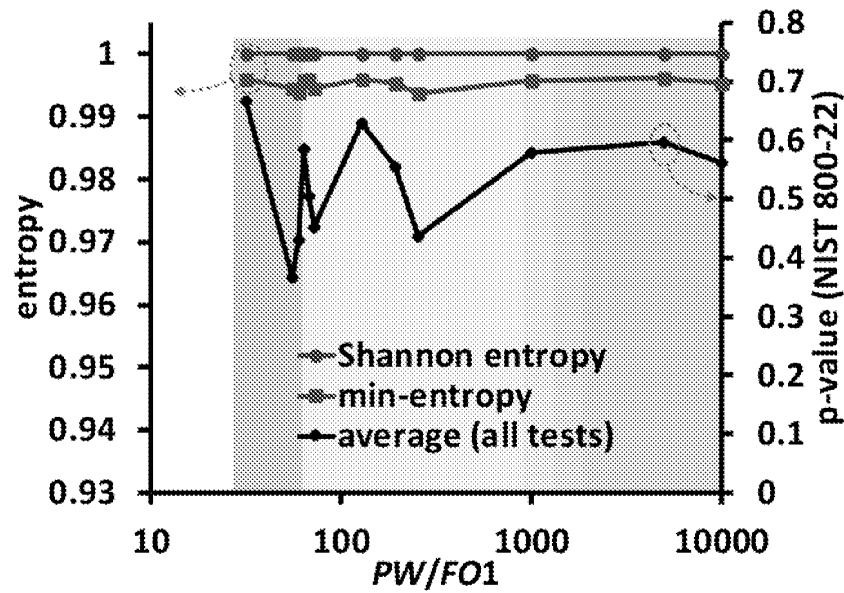


Figure 15

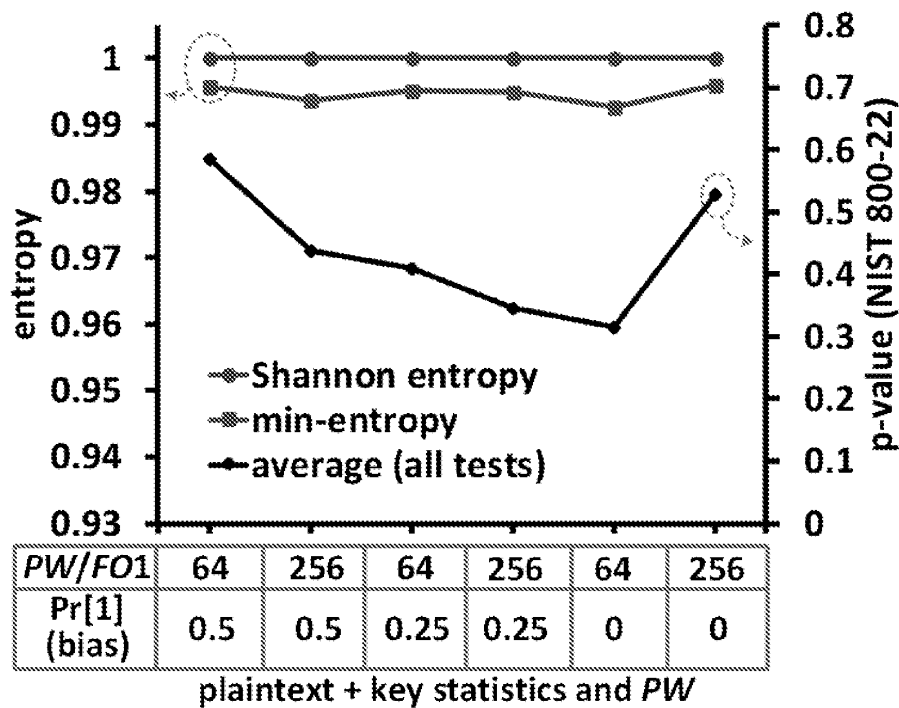


Figure 16

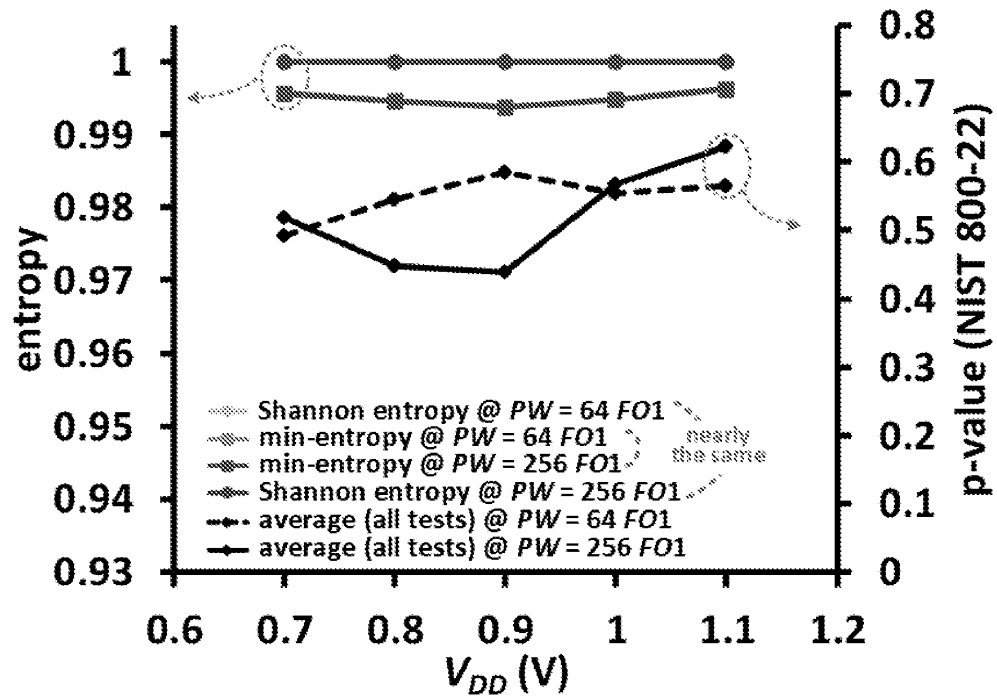


Figure 17

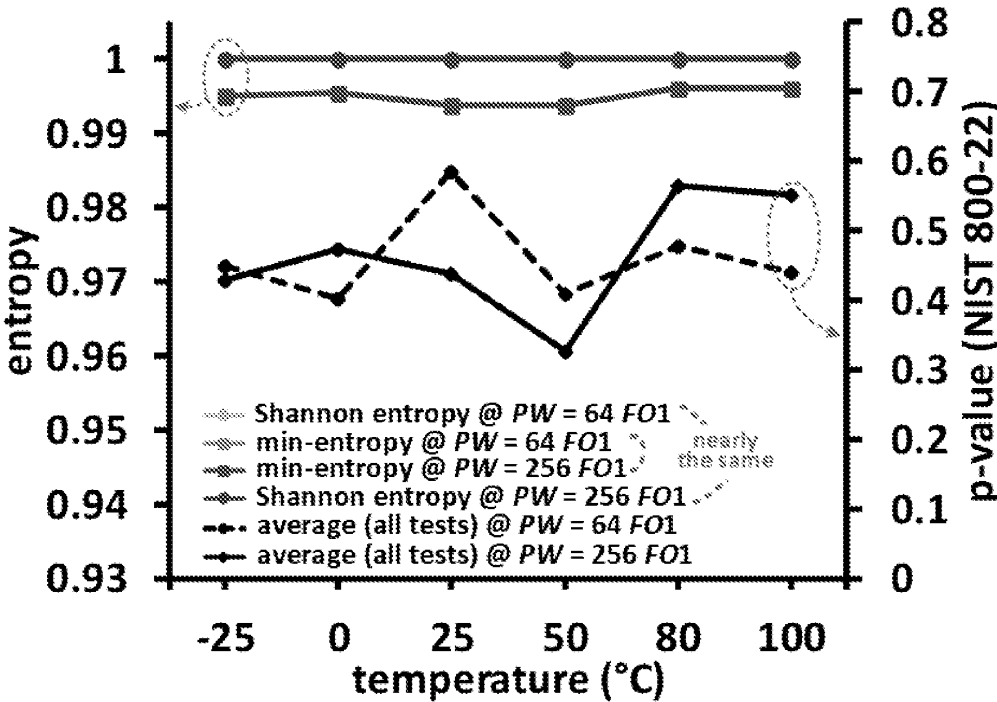


Figure 18

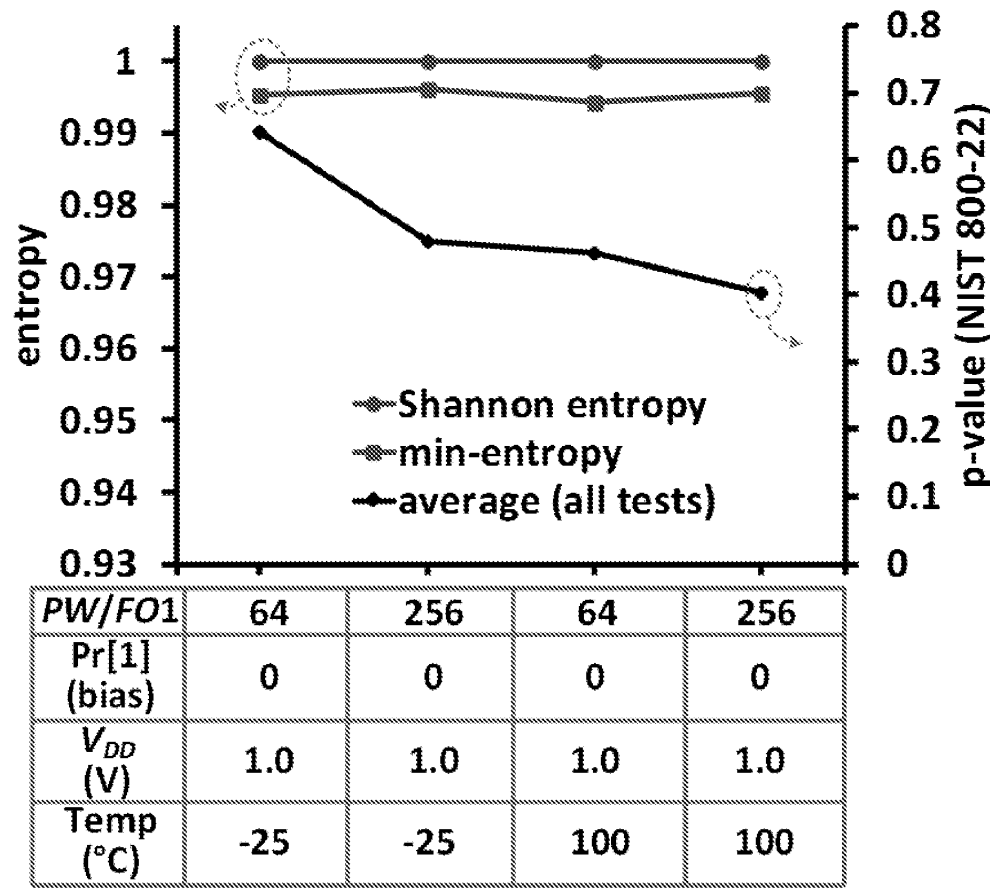


Figure 19(a)

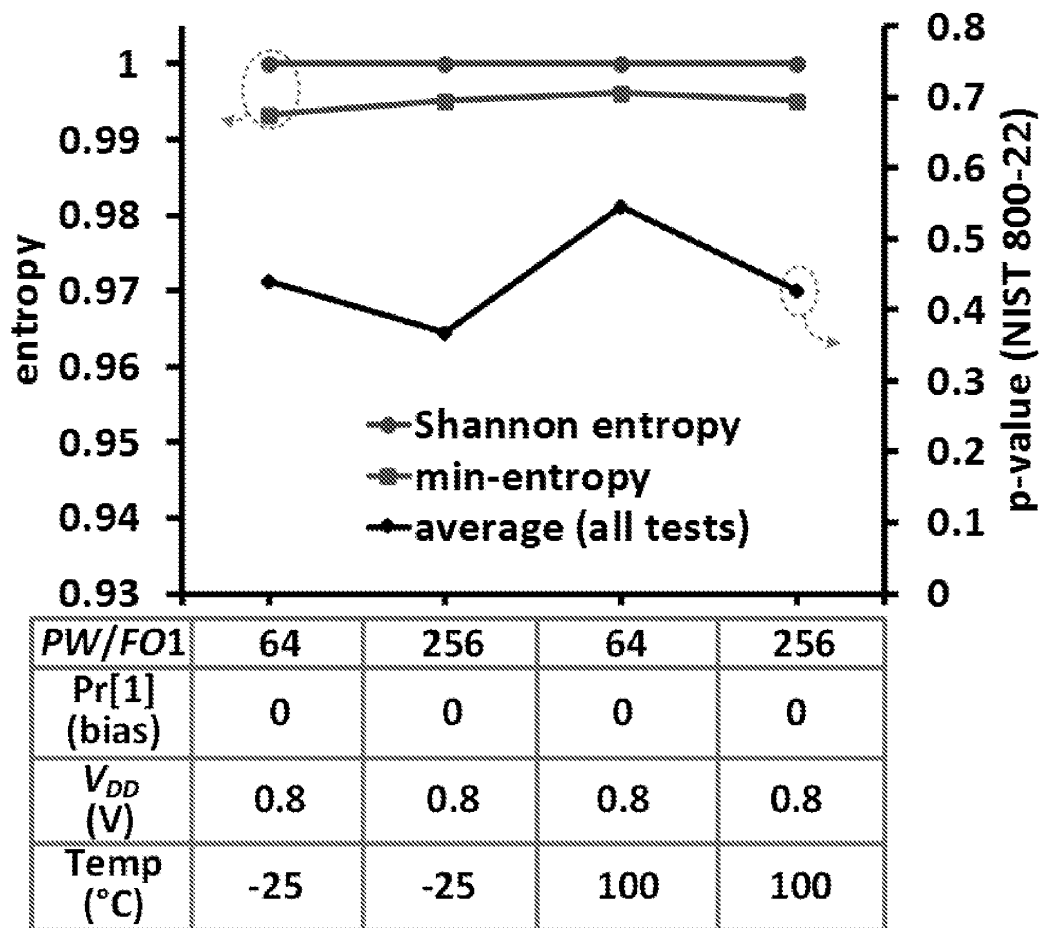


Figure 19(b)

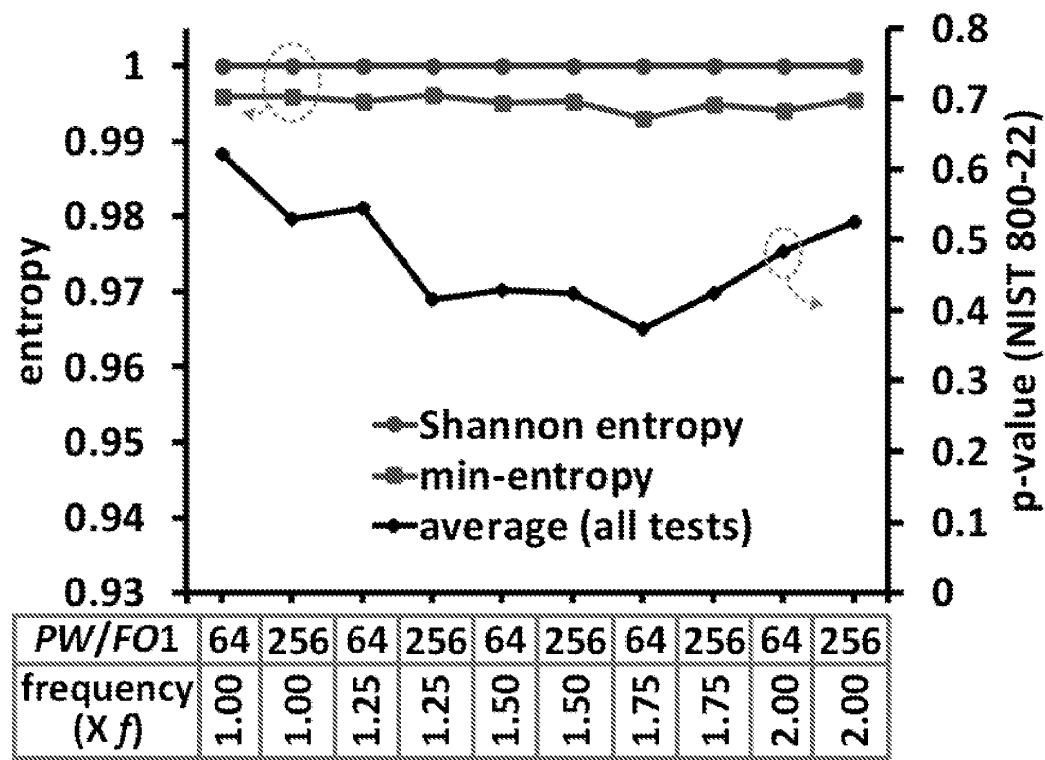


Figure 20

TABLE I. COMPARISON TABLE (BEST PERFORMANCE AND FAVORABLE FEATURE IN BOLD)

|                                                                    | This work                            | SSC-L 2020<br>[17]     | JSSC 2019<br>[3]      | VLSI 2018<br>[4] | JSSC 2017<br>[5]      | ISSCC 2017<br>[6]     | JSSC 2016<br>[11] | JSSC 2016<br>[7]      |
|--------------------------------------------------------------------|--------------------------------------|------------------------|-----------------------|------------------|-----------------------|-----------------------|-------------------|-----------------------|
| technology (nm)                                                    | 40                                   | 65                     | 14                    | 65               | 180                   | 65                    | 14                | 40                    |
| entropy source <sup>(a)</sup>                                      | M + J                                | J                      | M                     | M                | CM                    | J                     | M                 | J                     |
| calibration                                                        | <b>NO</b>                            | <b>NO</b>              | <b>YES</b>            | <b>YES</b>       | <b>NO</b>             | <b>NO</b>             | <b>YES</b>        | <b>YES</b>            |
| all-digital                                                        | <b>YES</b>                           | <b>NO</b>              | <b>YES</b>            | <b>NO</b>        | <b>NO</b>             | <b>NO</b>             | <b>YES</b>        | <b>YES</b>            |
| synthesizable                                                      | <b>YES</b>                           | <b>NO</b>              | <b>NO</b>             | <b>NO</b>        | <b>NO</b>             | <b>NO</b>             | <b>NO</b>         | <b>NO</b>             |
| $V_{DD}$ (V)                                                       | 0.7 - 1.1                            | 0.8 - 1.2              | 0.55 - 0.75           | 0.53 - 1.0       | 0.6 - 0.9             | 1.08 - 1.2            | 0.3 - 0.95        | 0.6 - 0.9             |
| temperature (°C)                                                   | -25 - 100                            | -20 - 70               | 70                    | -20 - 100        | -                     | -                     | -                 | -40 - 120             |
| # tested wafer lots                                                | <b>2</b>                             | -                      | -                     | -                | -                     | -                     | -                 | -                     |
| area (10 <sup>6</sup> F <sup>2</sup> )<br>(unified) <sup>(b)</sup> | <b>0.43</b><br>(YES)                 | 14.2<br>(YES)          | 10.8<br>(YES)         | 2.4<br>(NO)      | 6.5<br>(YES)          | <b>0.22</b><br>(NO)   | 5.55<br>(NO)      | 0.52<br>(NO)          |
| minimum energy<br>(pJ/bit)                                         | 2.5 <sup>(c)</sup><br>@ 0.7 V        | 6.9<br>@ 0.9 V         | 2.5<br>@ 0.65 V       | 2.58<br>@ 0.53 V | <b>0.3</b><br>@ 0.6 V | 35.5<br>@ 1.08 V      | 3.1<br>@ 0.4 V    | 11<br>@ 0.6 V         |
| energy efficiency<br>(Tbps/W) <sup>(d)</sup>                       | 0.4                                  | 0.145                  | 0.4                   | 0.388            | <b>3.33</b>           | 0.028                 | 0.523             | 0.091                 |
| max. throughput<br>(Mbps) <sup>(d)</sup>                           | 128                                  | 52                     | <b>1,480</b>          | 86               | 0.27                  | 9.9                   | 225               | 2                     |
| area efficiency<br>(Mbps/10 <sup>6</sup> F <sup>2</sup> )          | <b>299</b>                           | 3.66                   | 137                   | 35.8             | 0.04                  | 45                    | 40.5              | 3.82                  |
| NIST 800-90B IID<br>test pass                                      | <b>100%</b>                          | <b>100%</b>            | -                     | <b>100%</b>      | -                     | -                     | -                 | -                     |
| inherent obfuscation                                               | <b>YES</b>                           | <b>NO</b>              | <b>NO</b>             | <b>NO</b>        | <b>NO</b>             | <b>NO</b>             | <b>NO</b>         | <b>NO</b>             |
| frequency attack<br>robustness                                     | <b>YES</b><br>(0.3 V) <sup>(e)</sup> | <b>YES</b><br>(0.19 V) | N/A                   | N/A              | N/A                   | <b>YES</b><br>(0.4 V) | N/A               | <b>YES</b><br>(0.5 V) |
| unified functions                                                  | <b>TRNG +<br/>crypto</b>             | <b>TRNG +<br/>ADC</b>  | <b>TRNG +<br/>PUF</b> | -                | <b>TRNG +<br/>ADC</b> | -                     | -                 | -                     |

<sup>a</sup>. Entropy source (M - metastability, J - jitter, CM - chaotic map)

<sup>b</sup>. Area includes the unified functions, [3] requires 750 additional gates on off-chip FPGA for entropy extraction

<sup>c</sup>. XOR-based entropy extractor accounts for 0.2% energy and 0.02·10<sup>6</sup> F<sup>2</sup> area overhead (off-chip). The clock generator is invariably ignored in the literature and hence not considered in this table. In this work, the tunable clock pulsewidth generator in the 10–64 FO1 range entails a marginal energy (4%) and area increase (2.3%)

<sup>d</sup>. Energy efficiency is reported at the voltage that minimizes energy, maximum throughput is reported at the highest supply voltage

<sup>e</sup>. Higher amplitude and frequency for power supply frequency injection attack are limited by testing setup (i.e., the TRNG might be more robust than claimed)

Figure 21

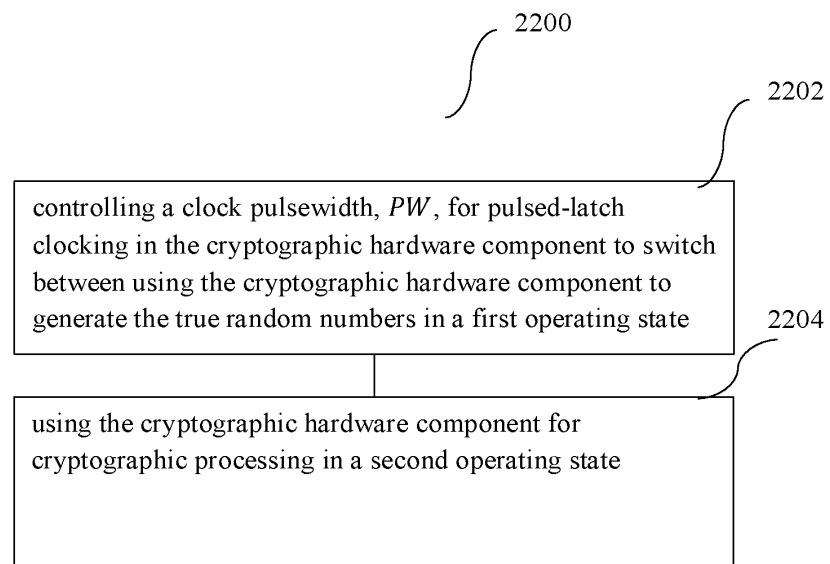


Figure 22