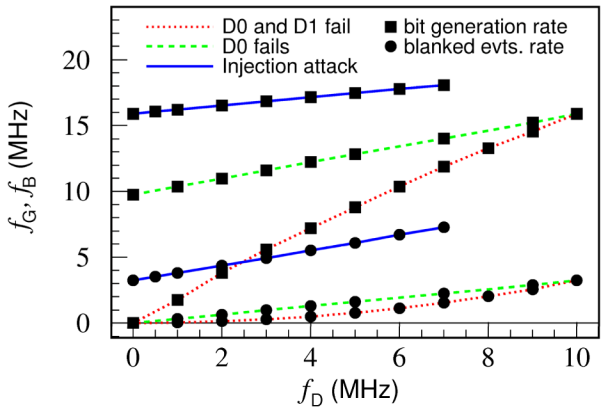

Fig. 8. Bit generation rate f_G (quadratic dots) and blanked events rate f_B (round dots) as functions of detection rates in three failure and attack scenarios (see the text). Both rates are sensitive to irregular operation of the RNG this allowing for robust monitoring and failure/attack detection.

We see that both generation (f_G) and blanked events (f_B) rates are quite sensitive to irregular operation of the RNG with a small advantage of f_G for scenario (*i*) and f_B for scenario (*iii*), whereas either is an equally good measure for scenario (*ii*). In the failure scenarios (*i*) and (*ii*) both parameters (f_G, f_B) drop below normal values whereas in the attack scenario (*iii*) both measures rise above their normal values. We thus have two measures, either of which (but preferably both) can be used to robustly alert malfunction of the COMBO RNG even at levels at which randomness is not noticeably compromised.

6. Conclusion

A RNG based on quantum effects in photonic emission and detection is presented. A mathematical framework for estimation of randomness quality based on simple measurements has been developed. The RNG is unique in several aspects: (1) the method of extraction of random bits simultaneously uses both spatial and temporal quantum information contained in the system; (2) the RNG is robust against hardware failure and signal injection attack in the sense that up to some threshold levels of detector failure or attack frequency randomness is virtually intact; (3) malfunction of the RNG, due to detector failure or signal injection, can be robustly detected at levels at which randomness is not significantly affected thus enabling protection of integrity of generated random bits. It is also shown that generated numbers pass the NIST Statistical Test Suite (STS) without the need for any further post-processing. Having in mind that partial detector failure scenario is identical to an initial or aging-related difference between detectors, we conclude that COMBO RBG is also robust to initial components variation and aging, which makes it a good candidate for mass-production or chip-level QRNG technology.

Acknowledgments

This work was supported by Fulbright program (academic year 2010/2011), Ministry of Science Education and Sports of Republic of Croatia (contract Nr. 098-0352851-2873). Extensive numerical simulations and randomness tests were made at Center for Scientific Computing UC Santa Barbara (contract Nr. NSF-CNS-0960316) and University Computing Centre (SRCE) of University of Zagreb.

#231845 - $15.00 USD Received 5 Jan 2015; revised 8 Mar 2015; accepted 24 Mar 2015; published 24 Apr 2015