

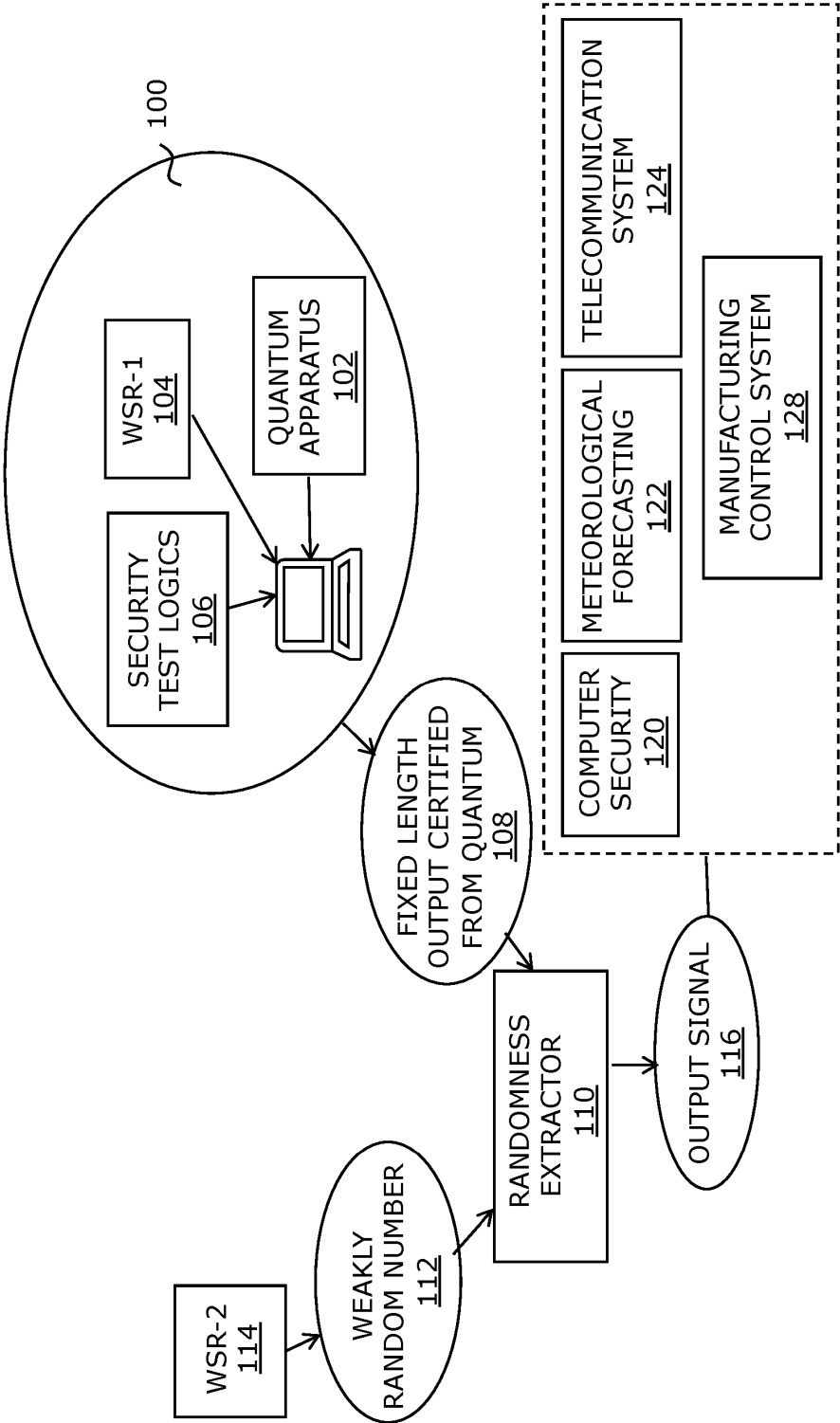


FIG. 1

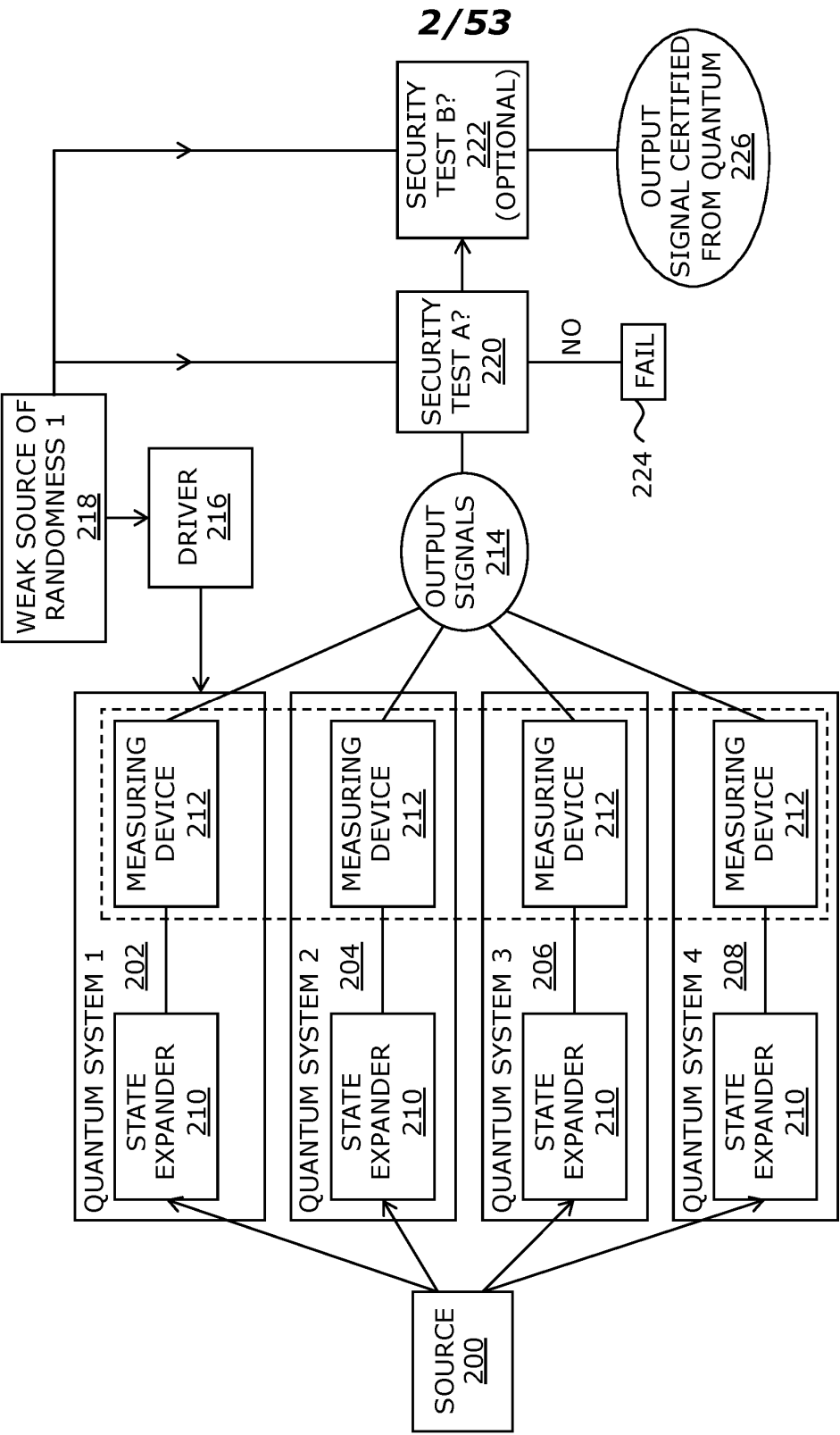


FIG. 2A

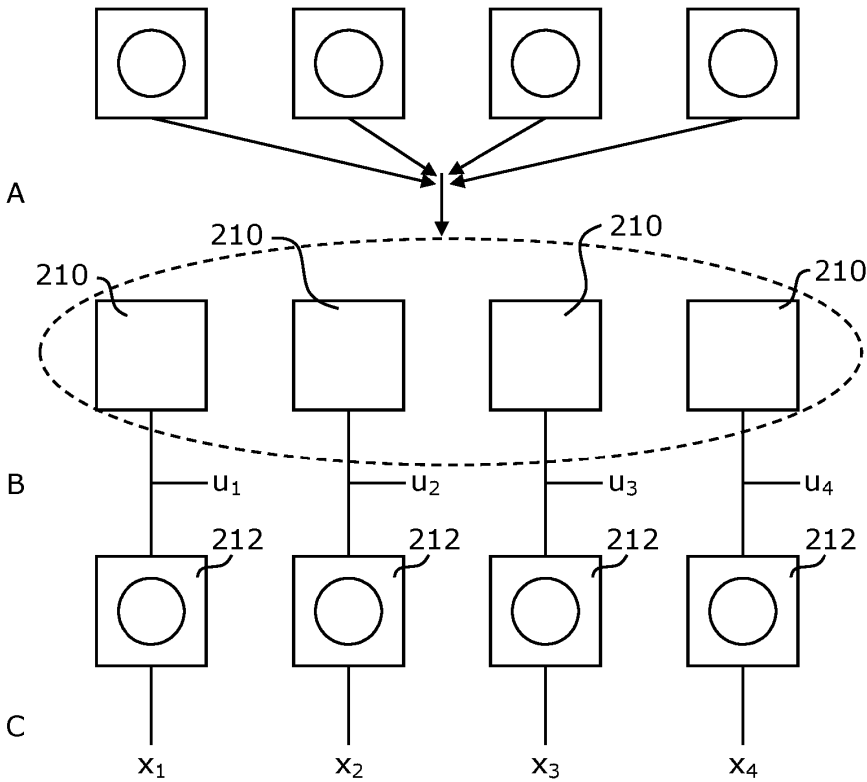
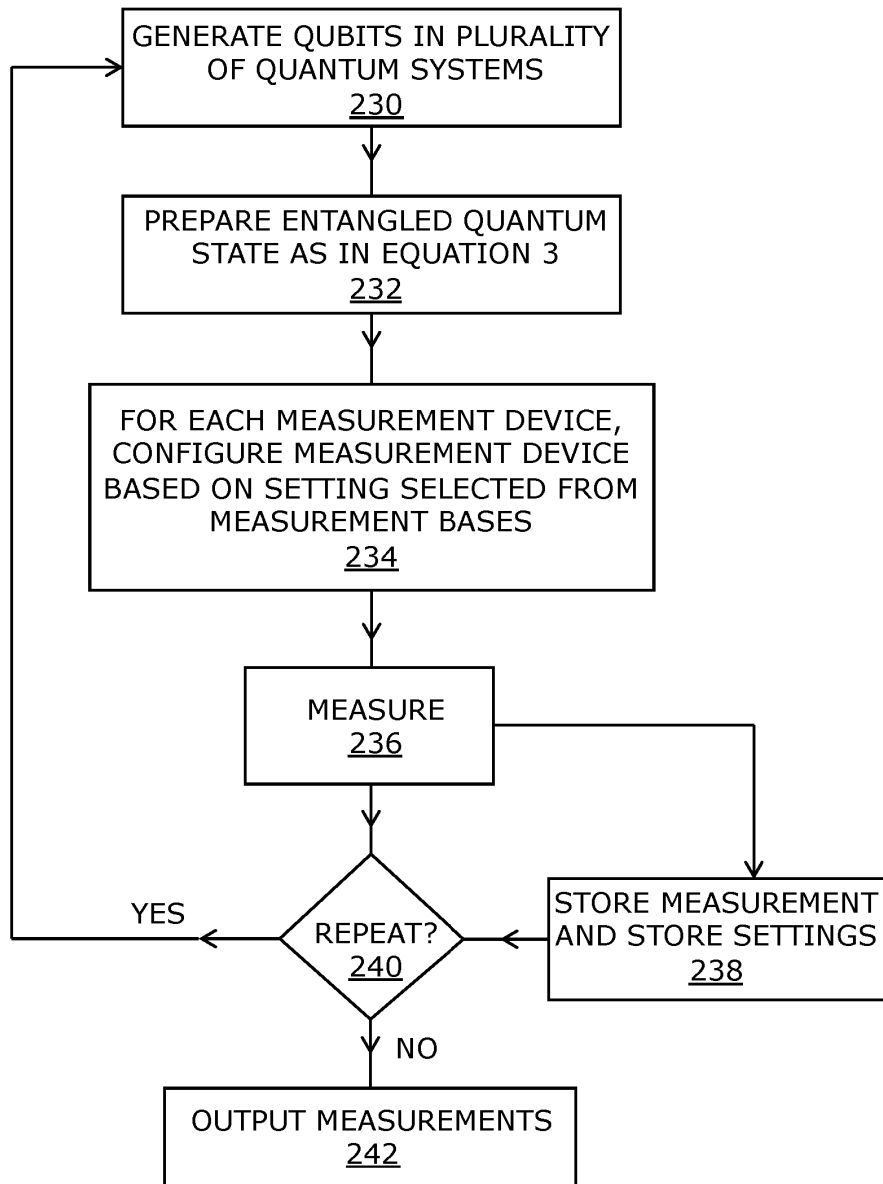


FIG. 2B

4/53**FIG. 2C**

5/53

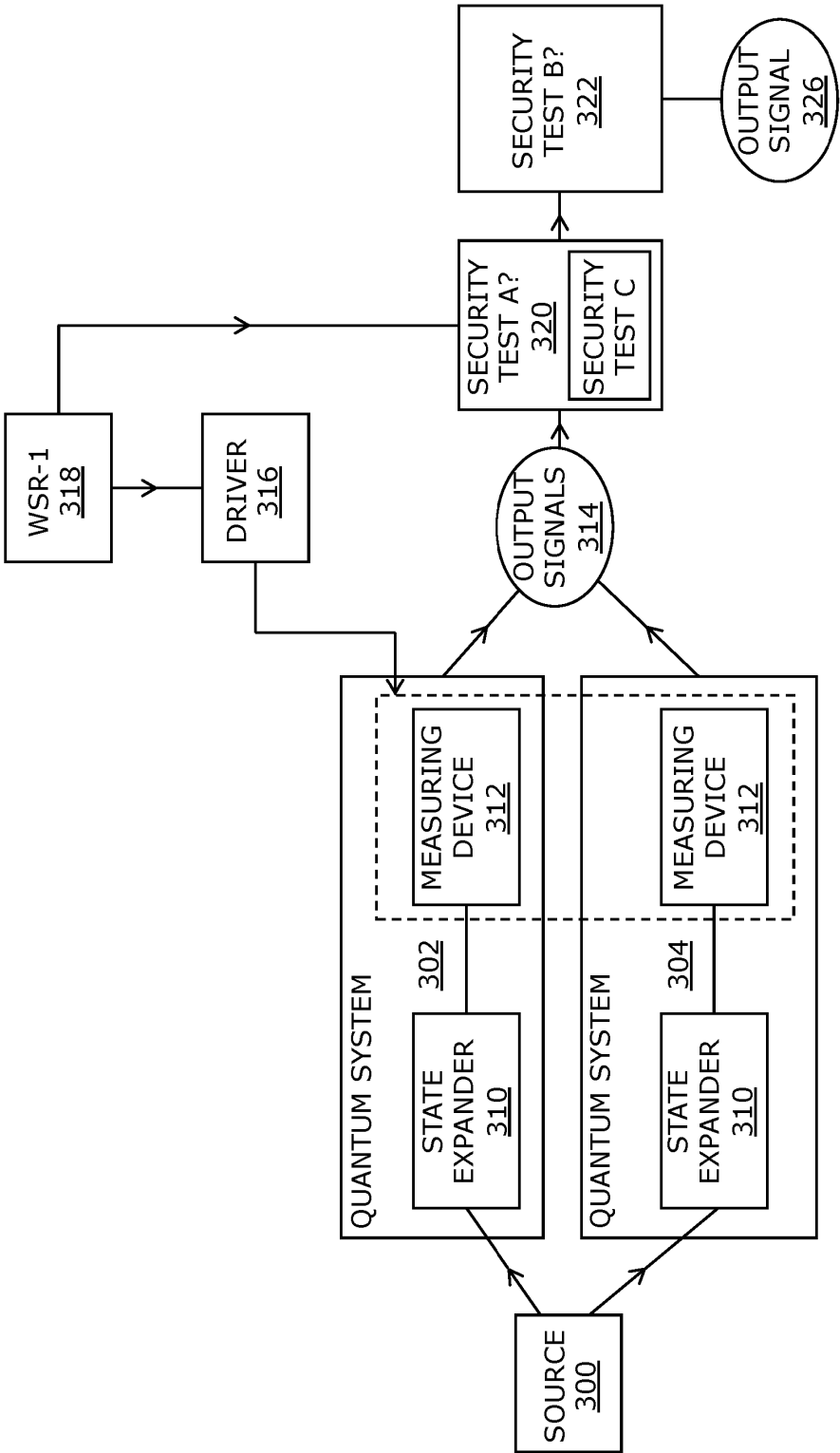


FIG. 3A

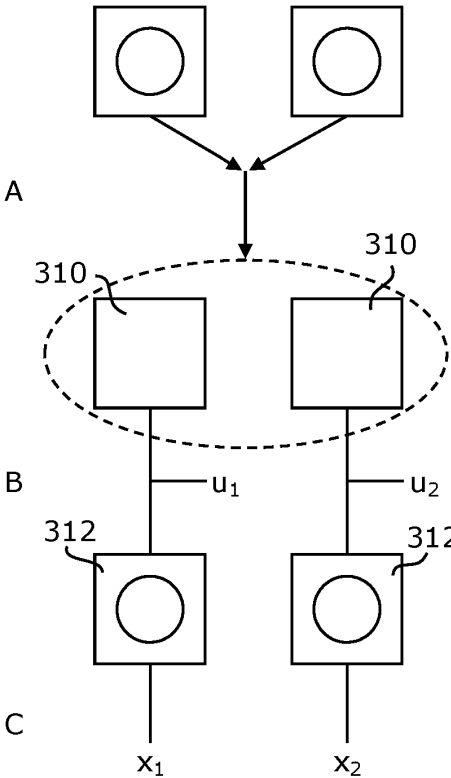
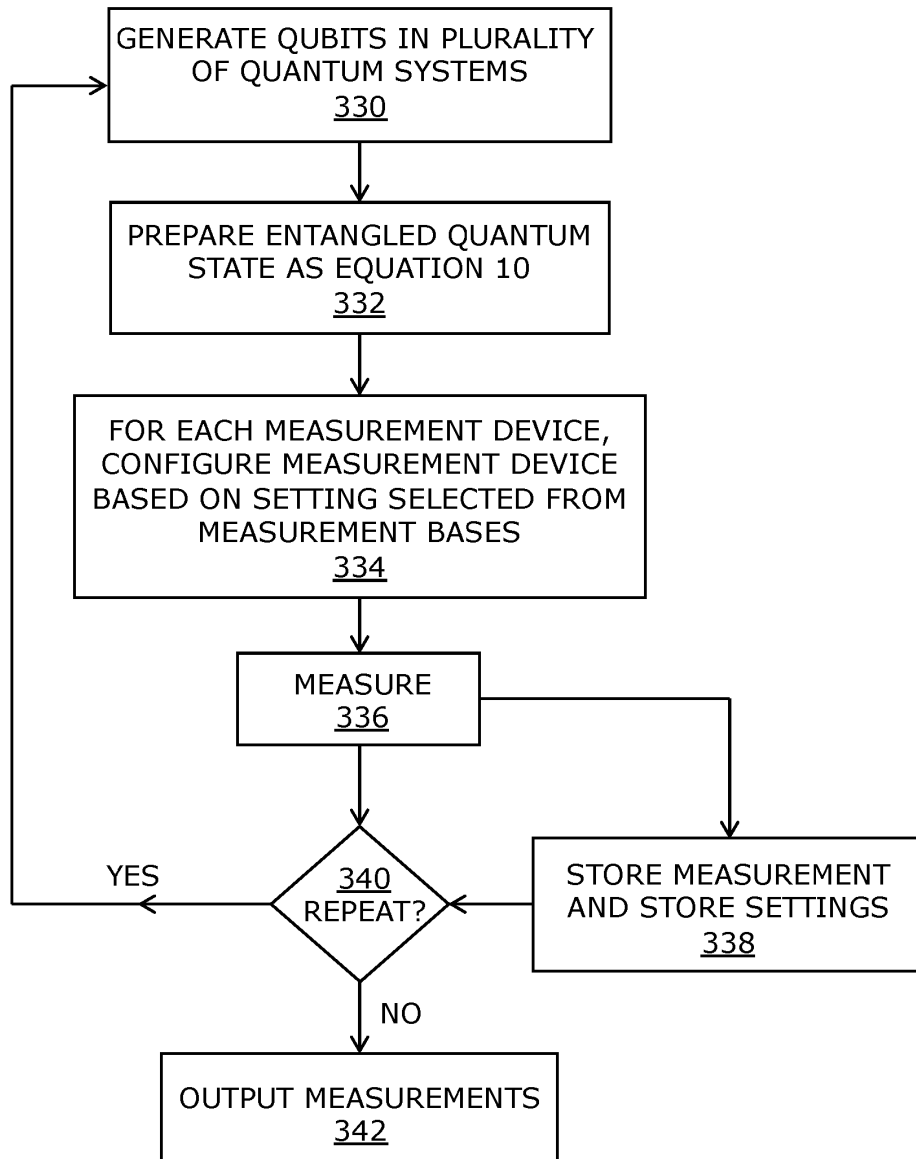
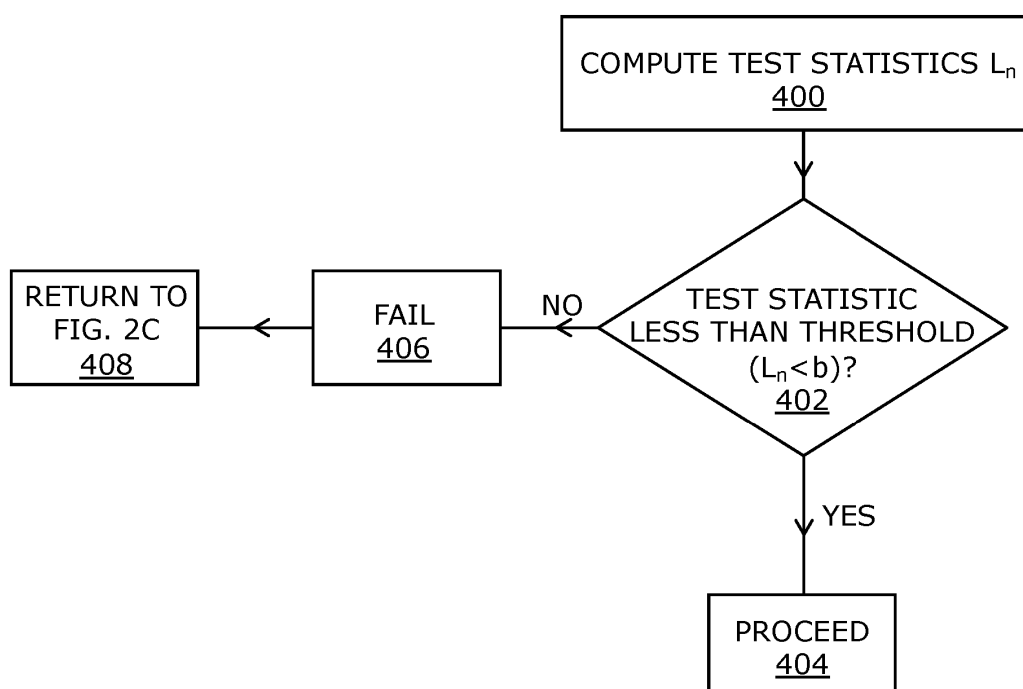
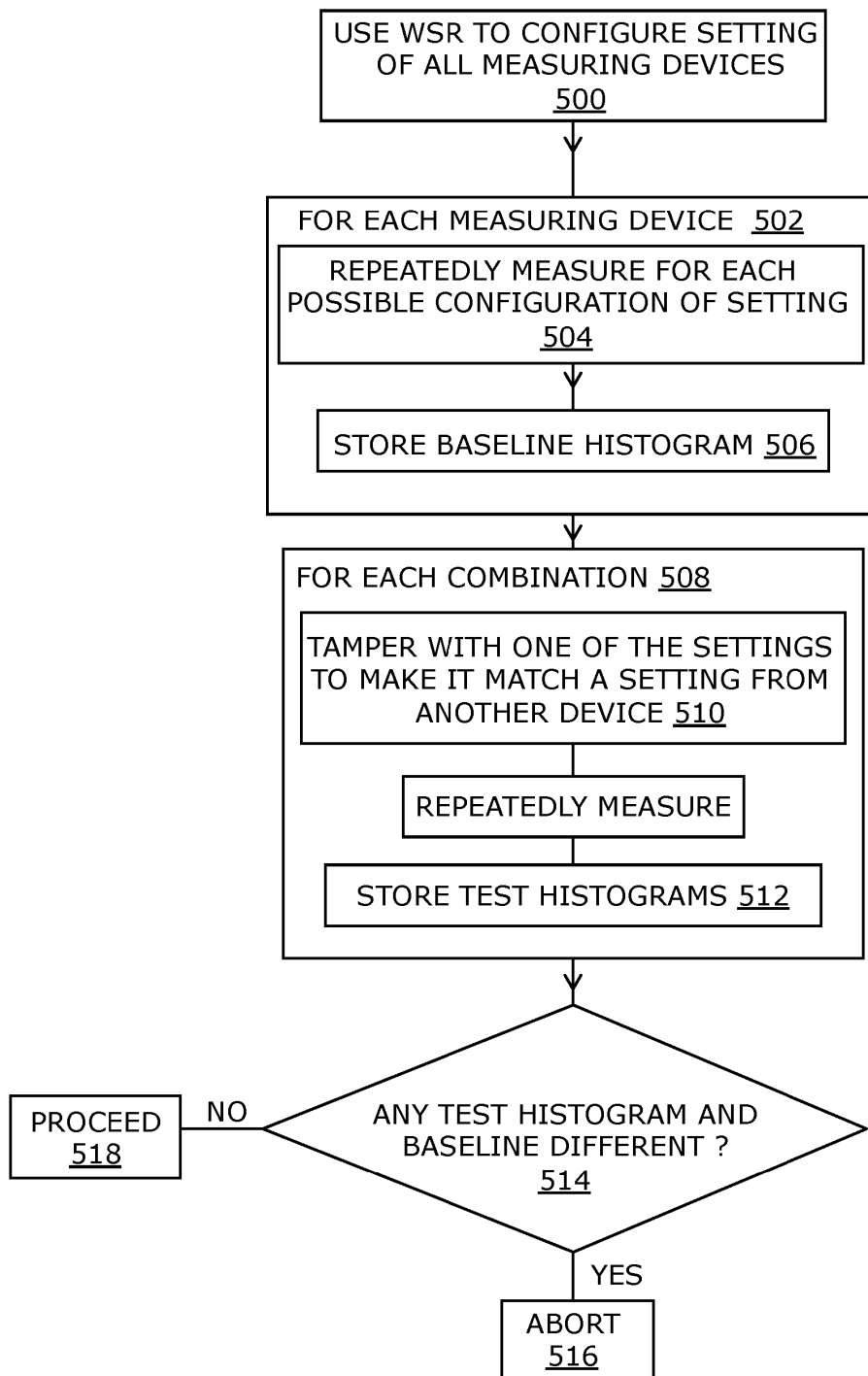
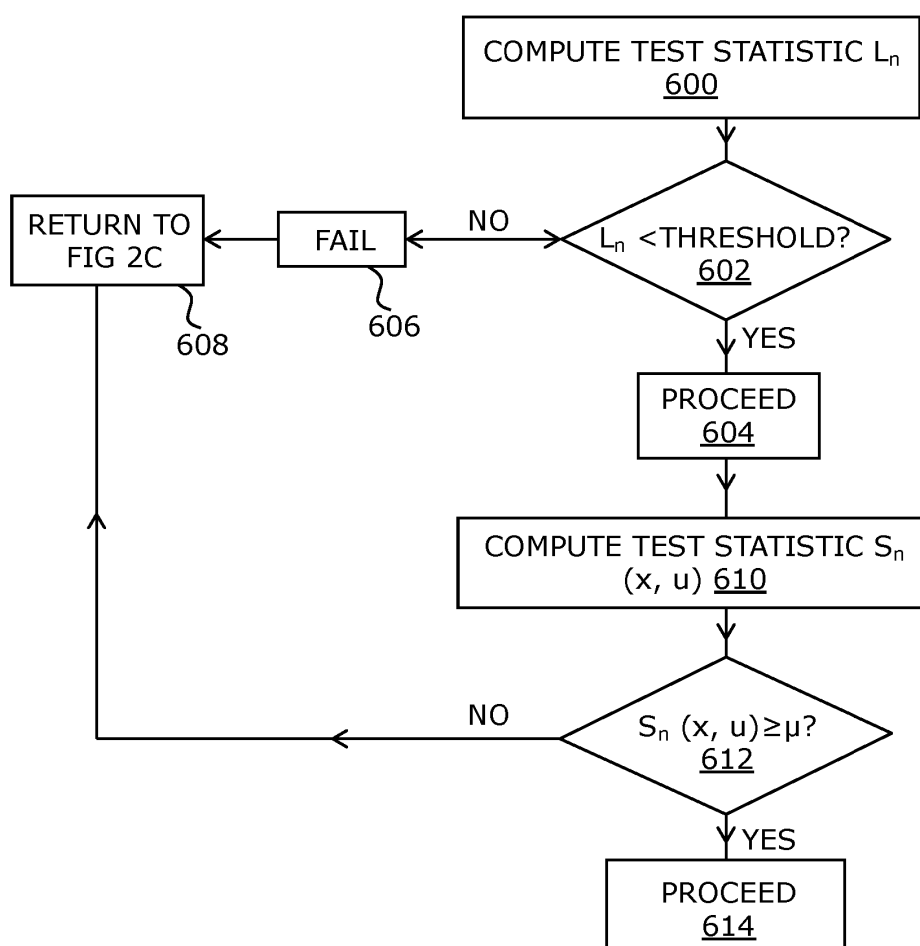


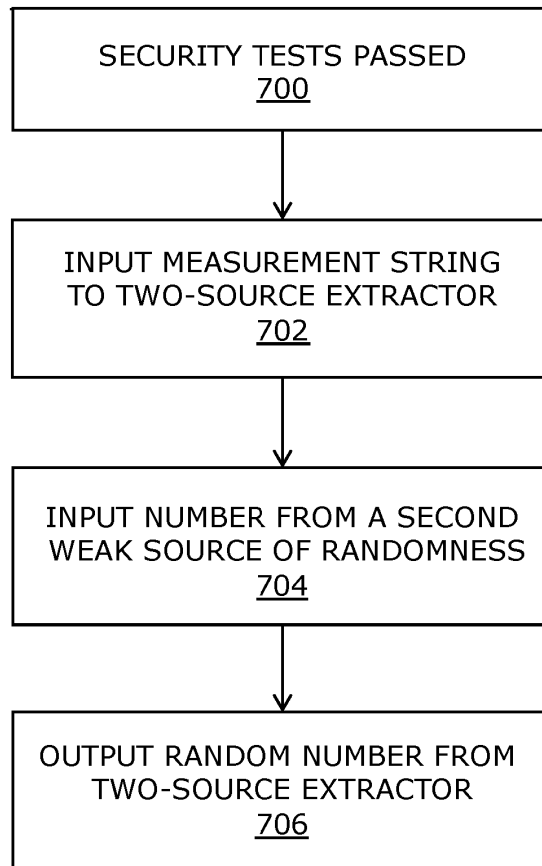
FIG. 3B

7/53**FIG. 3C**

8/53**FIG. 4**

9/53**FIG. 5**

10/53**FIG. 6**

11/53**FIG. 7**

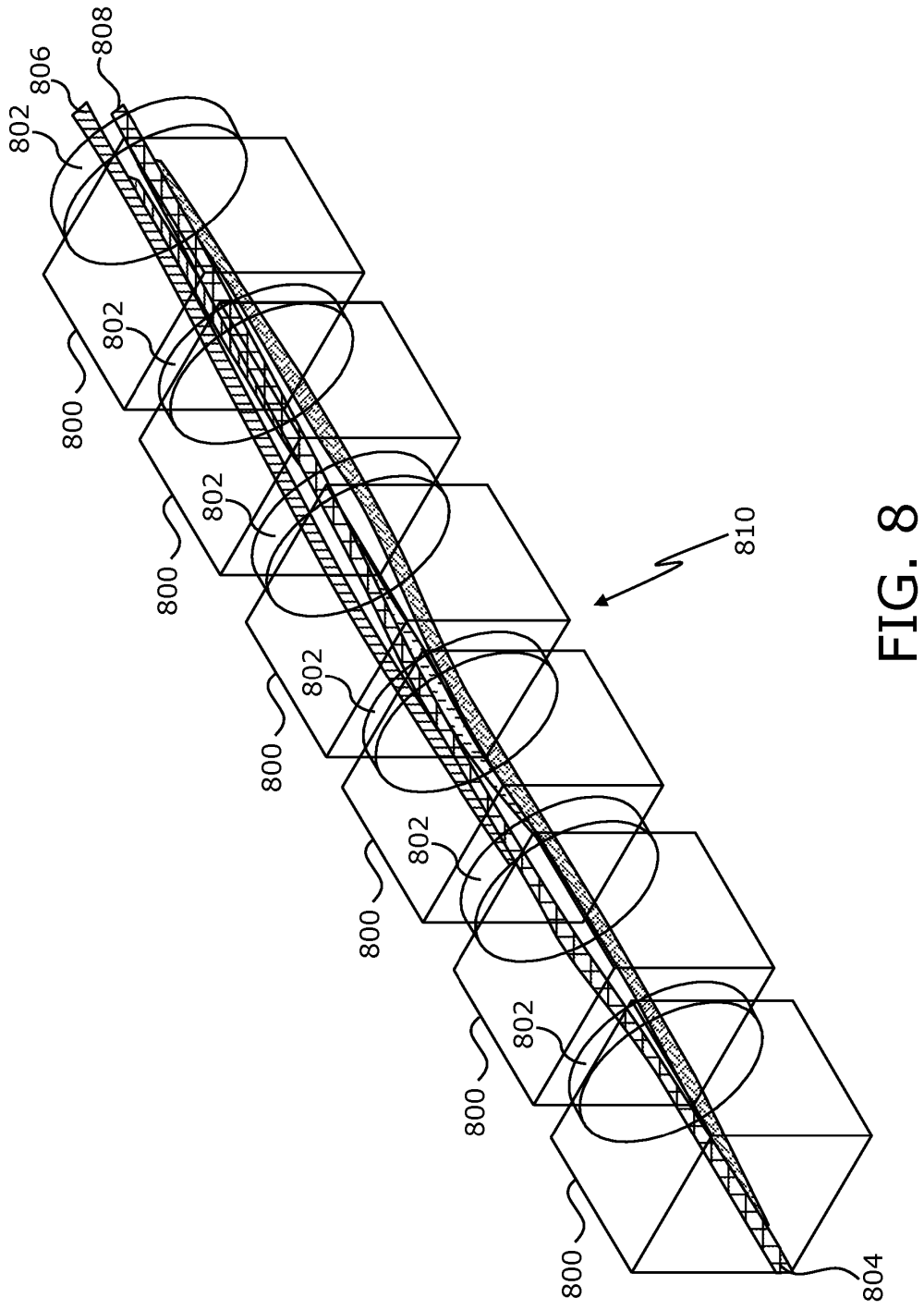


FIG. 8

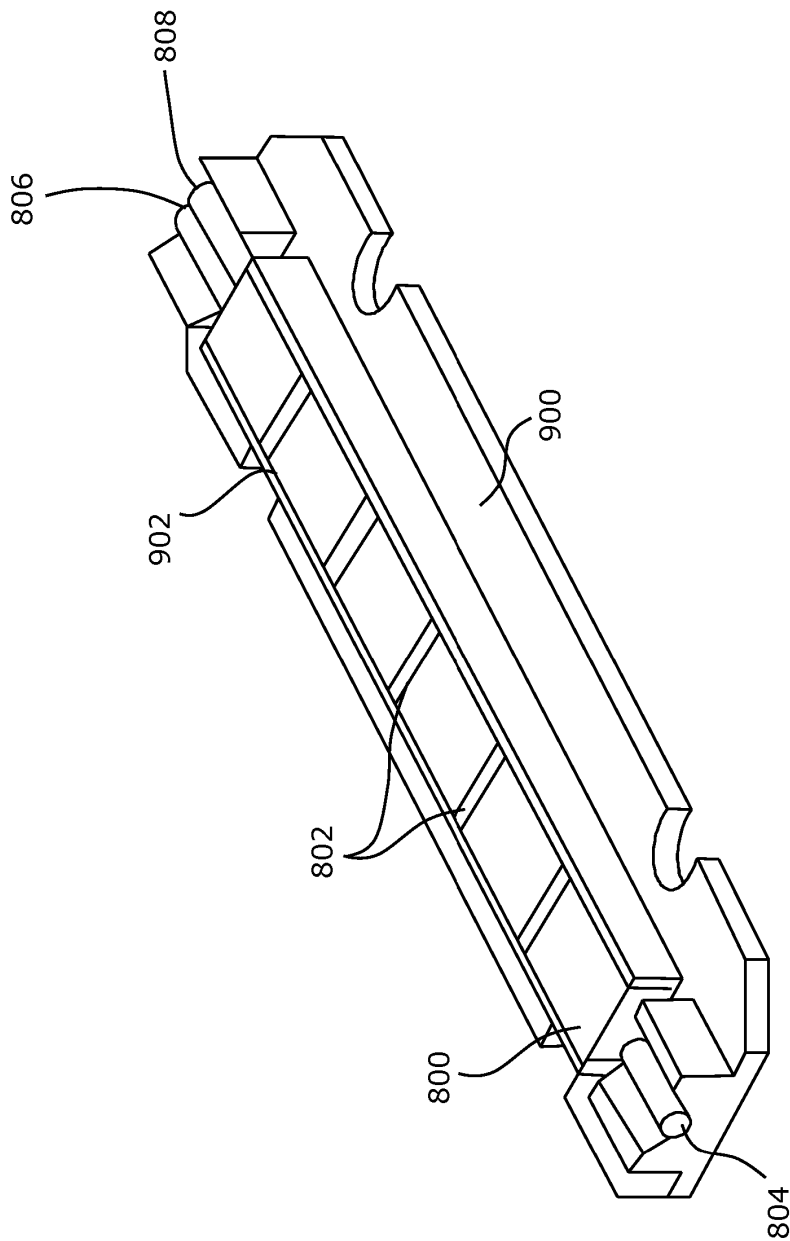


FIG. 9

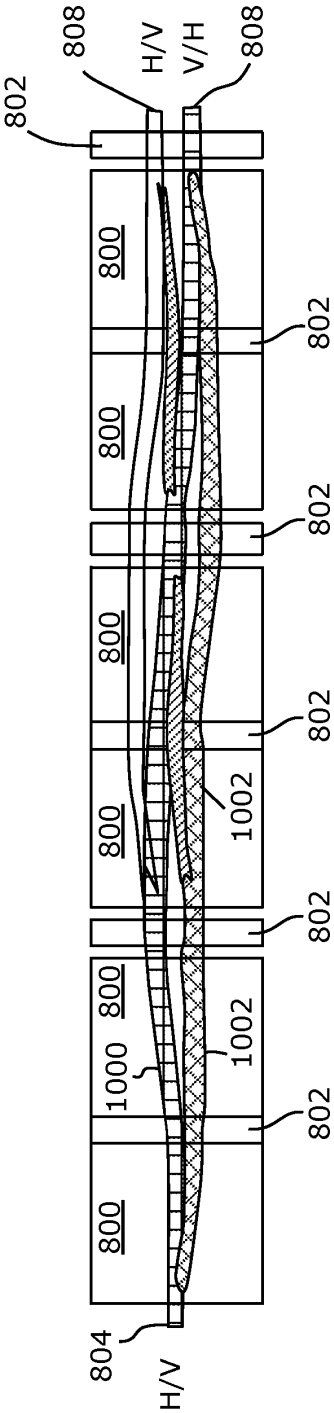


FIG. 10

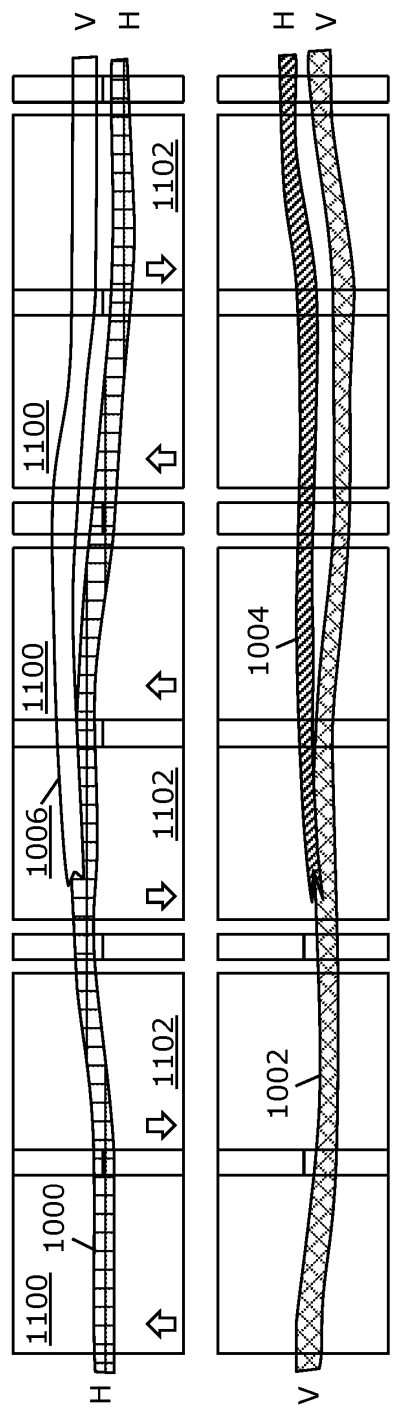


FIG. 11A

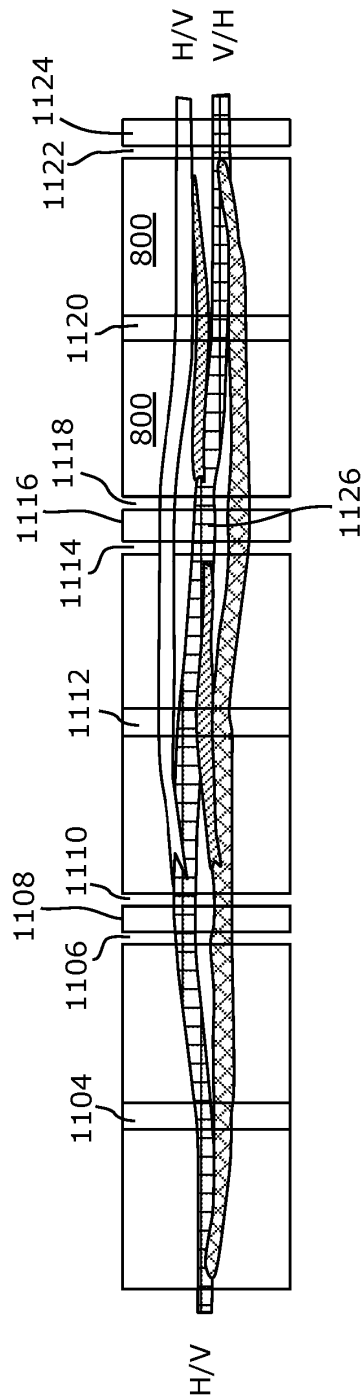


FIG. 11B

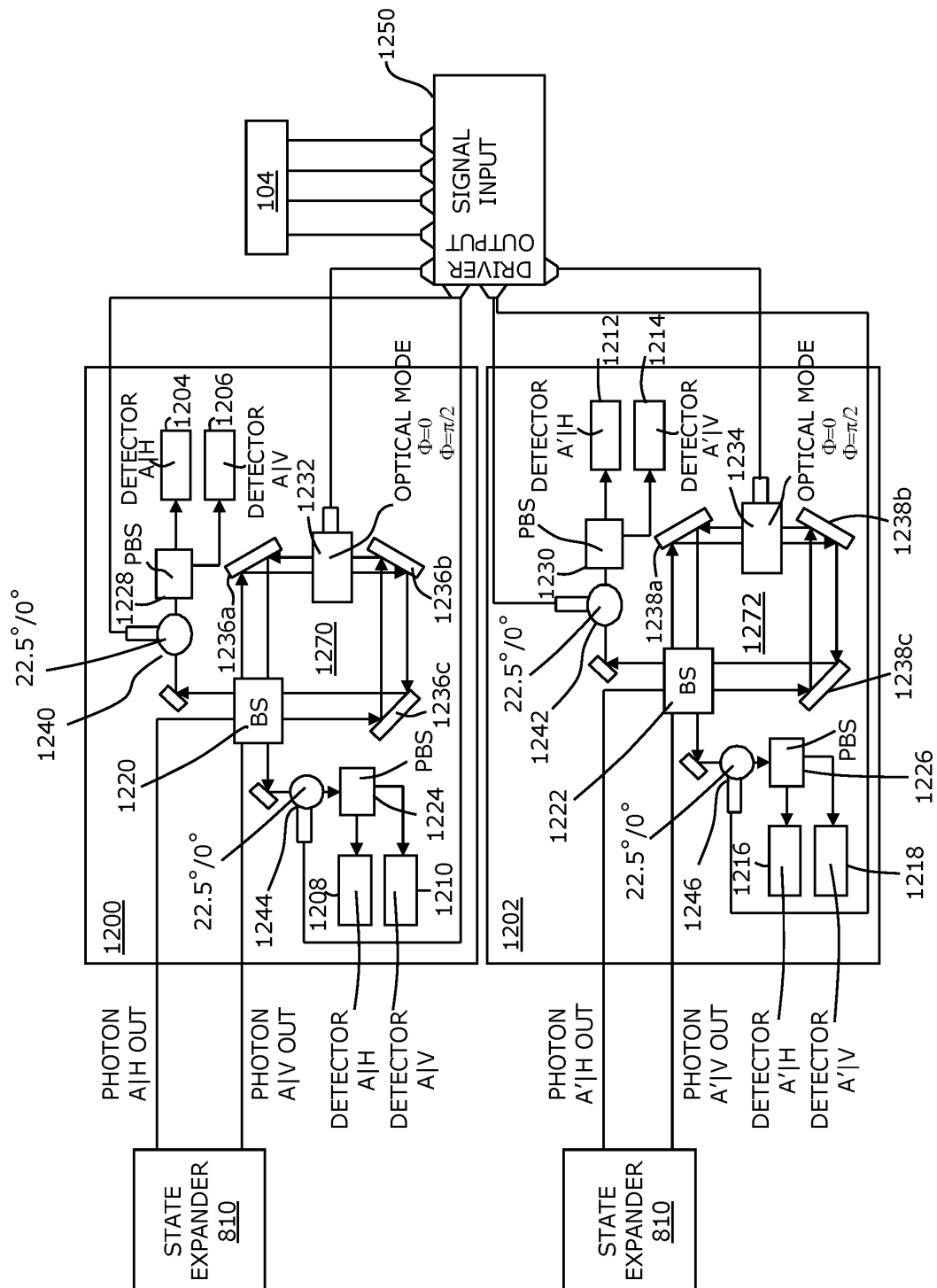


FIG. 12

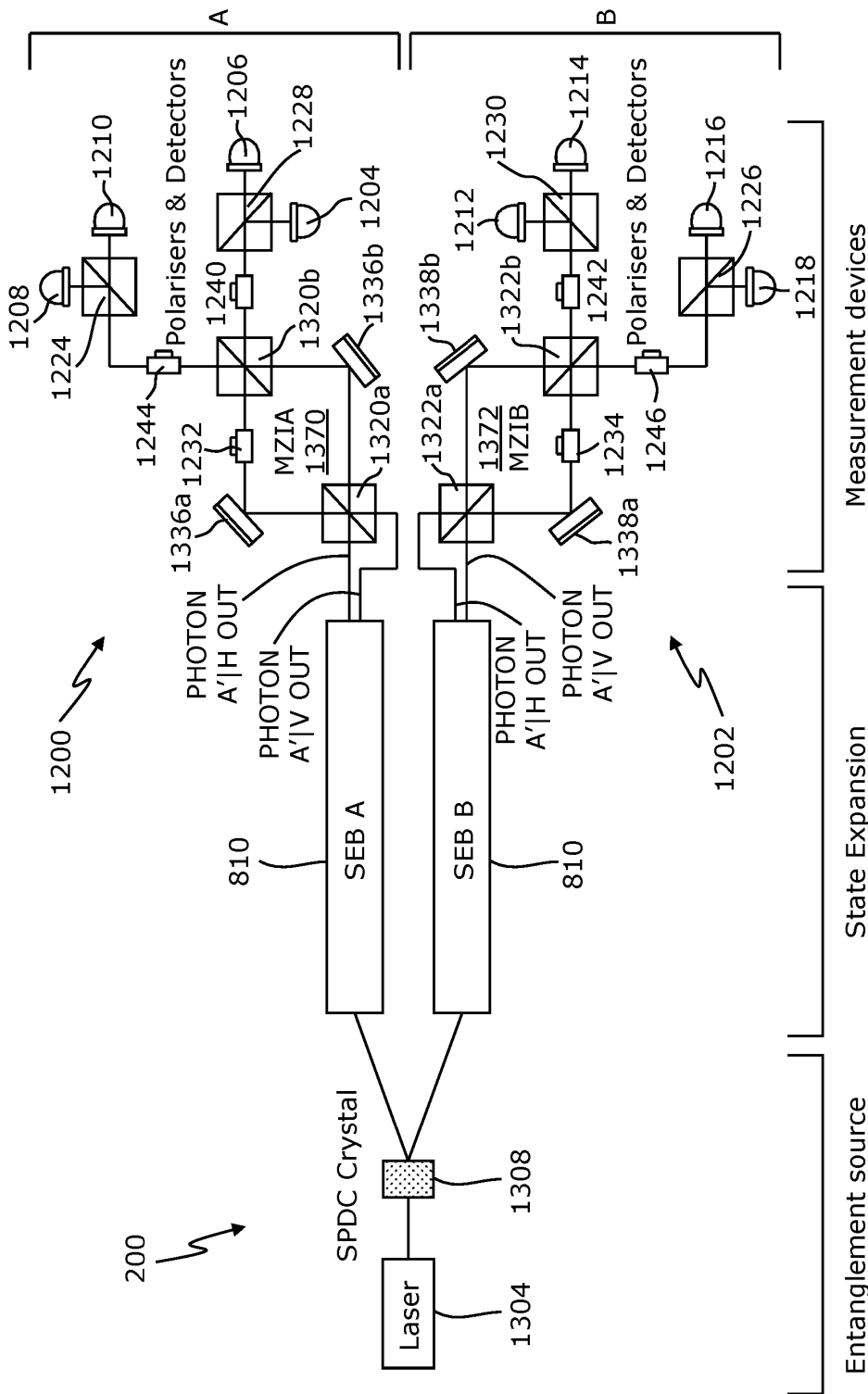


FIG. 13A

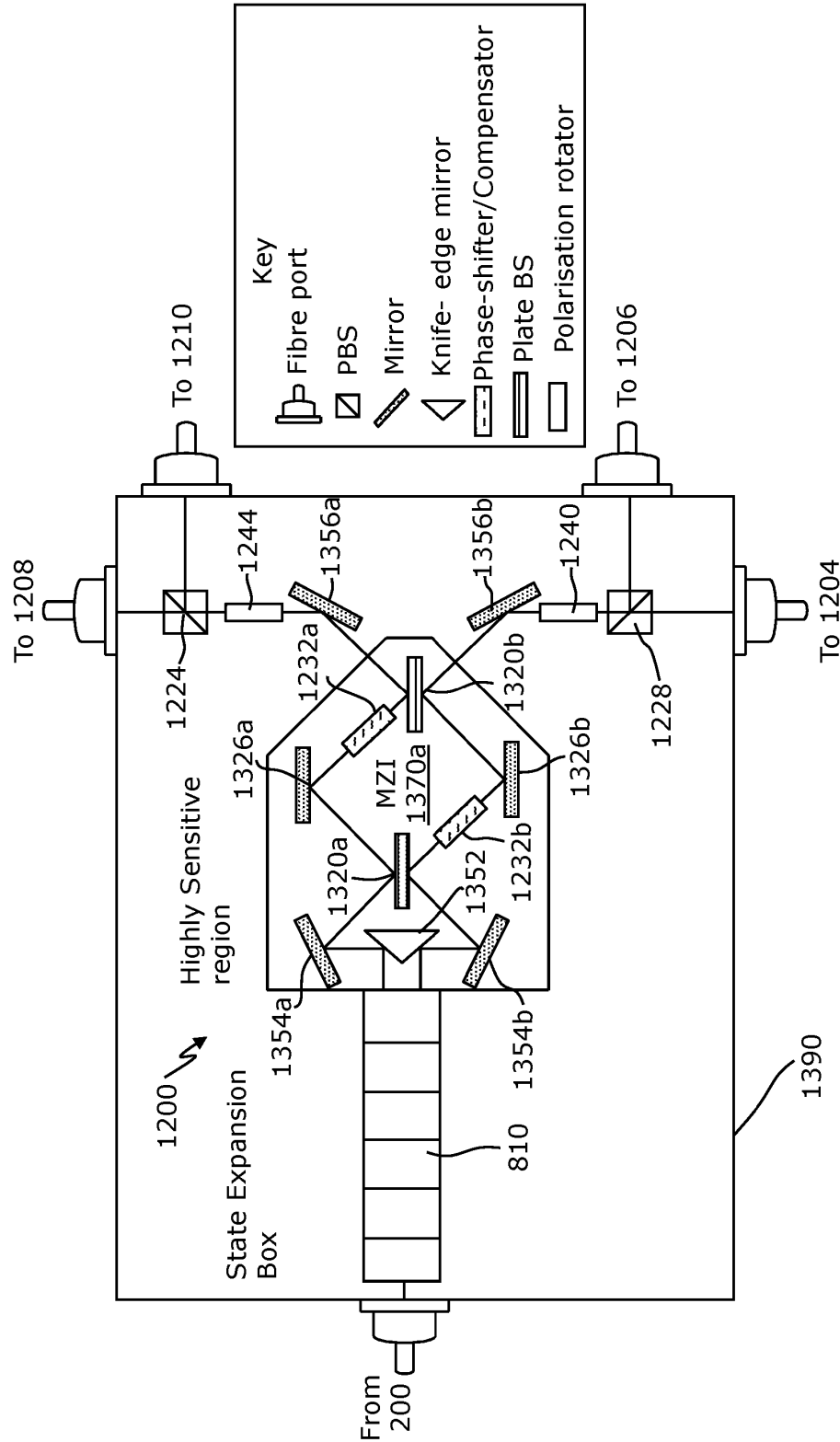


FIG. 13B

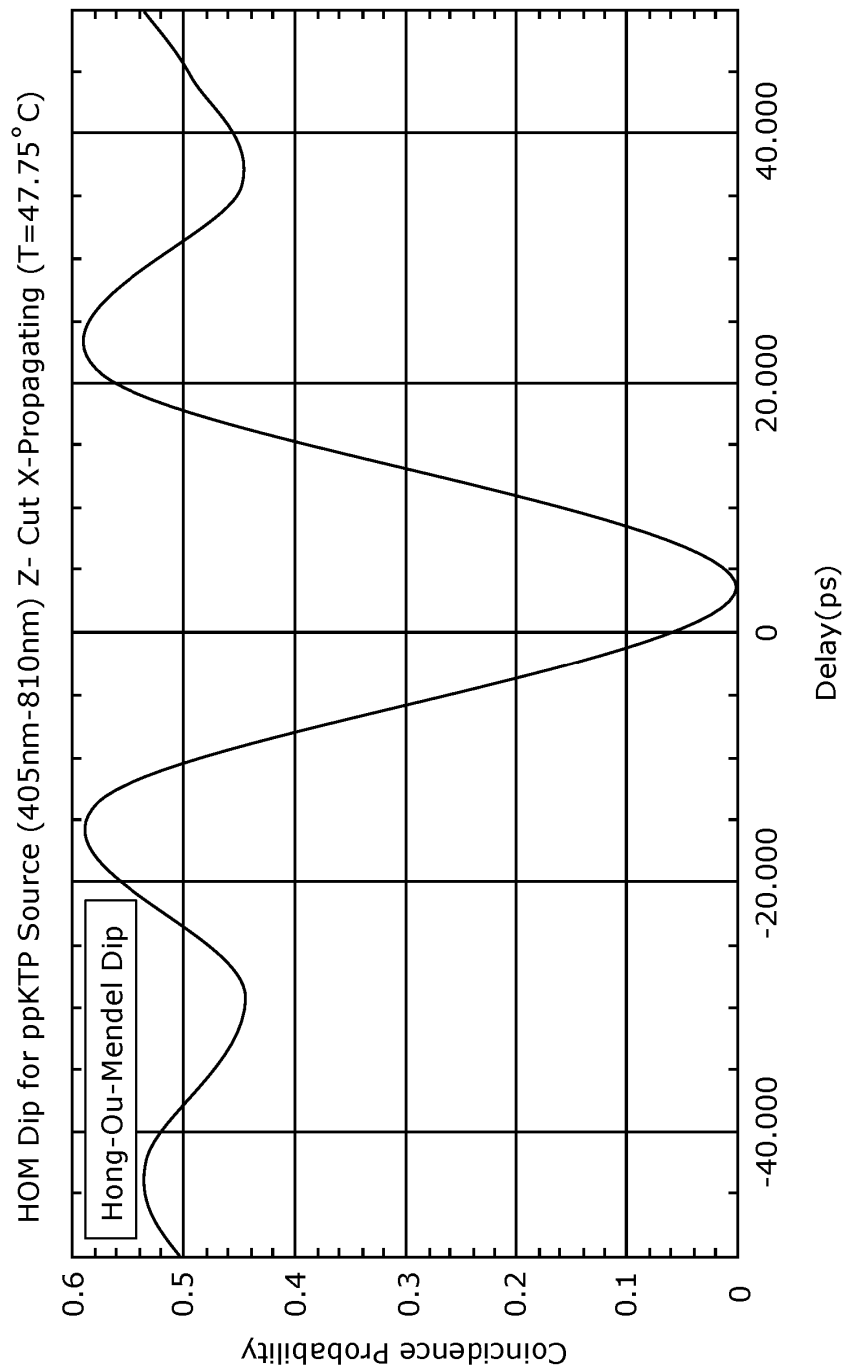


FIG. 14

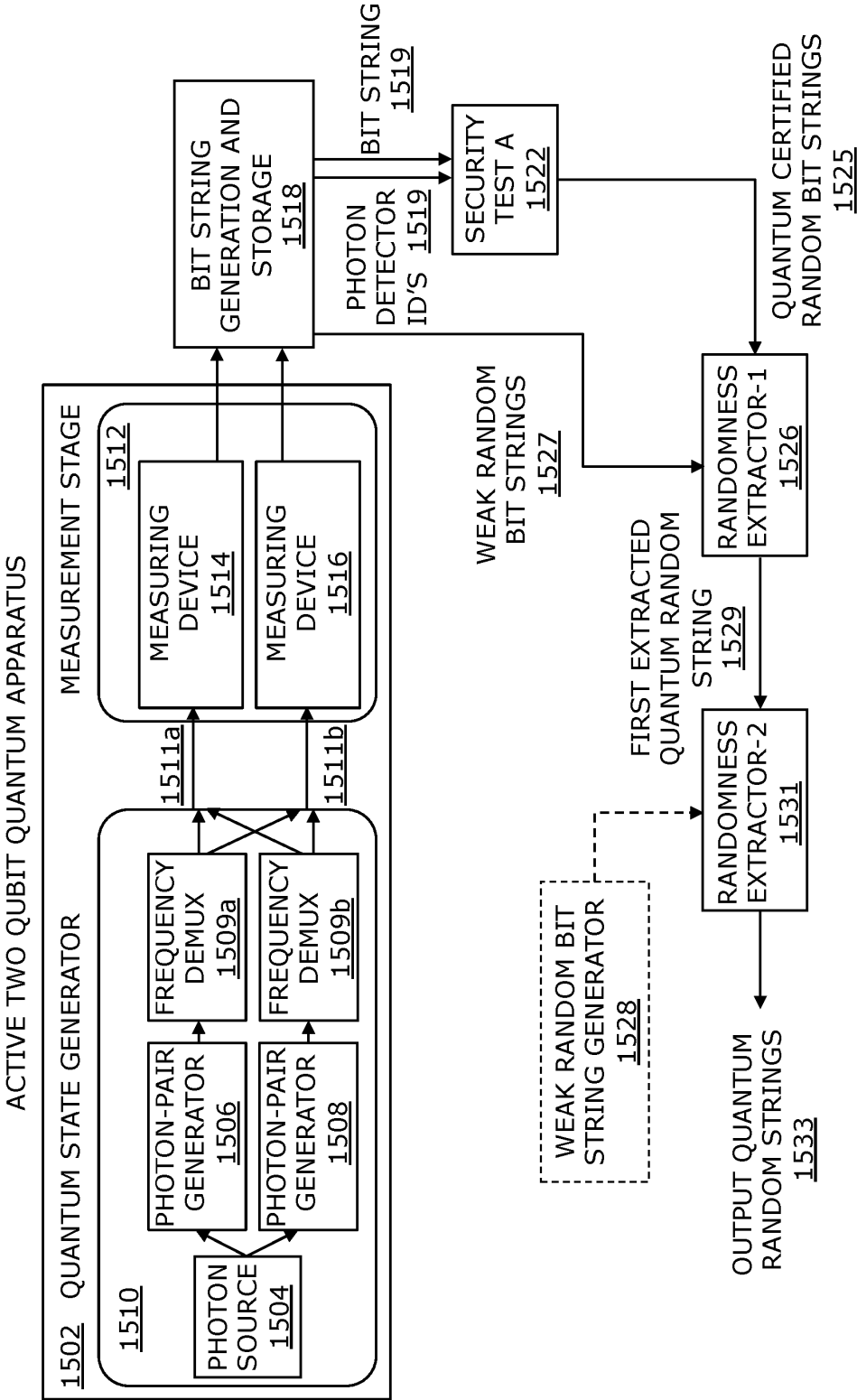
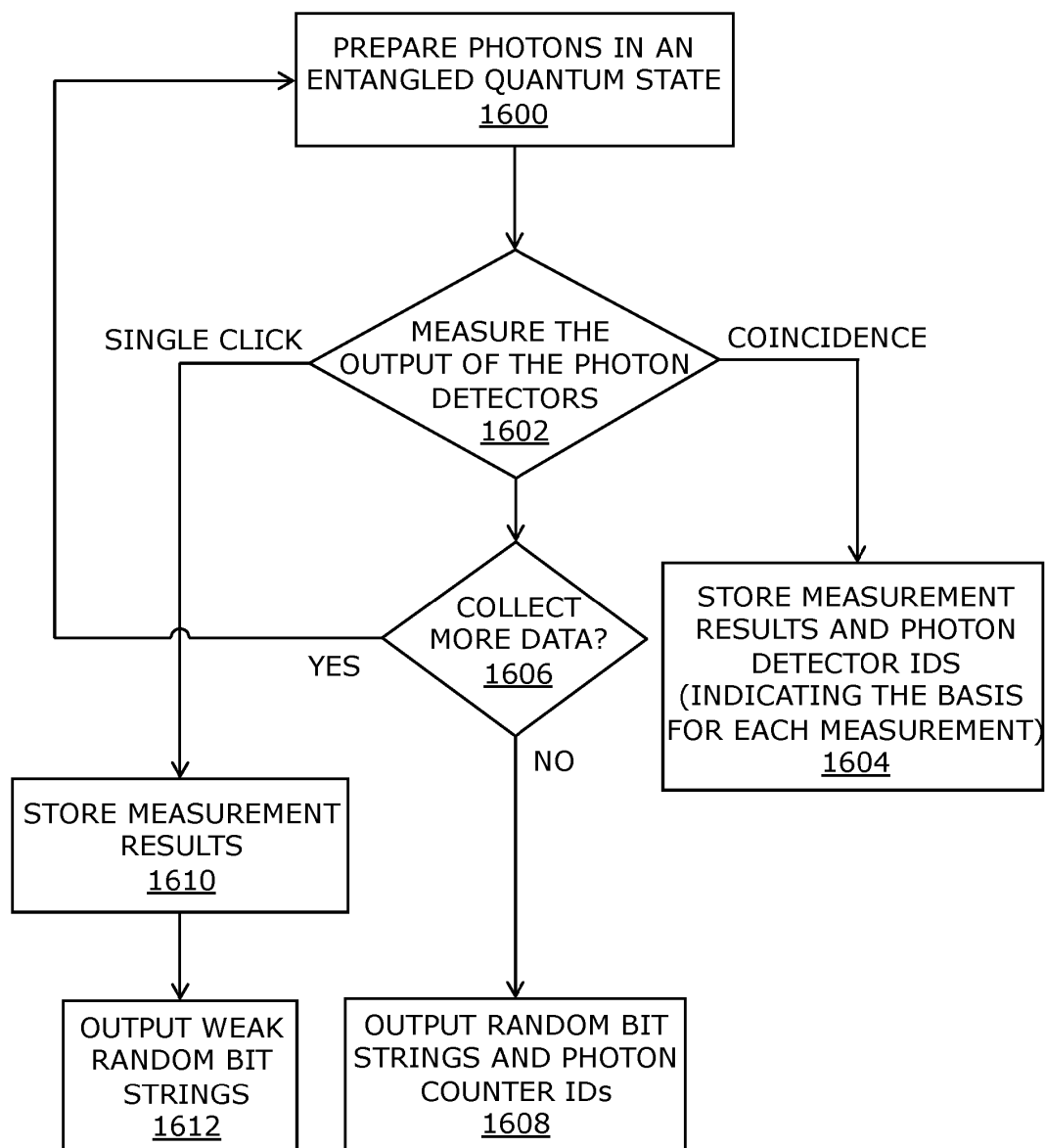
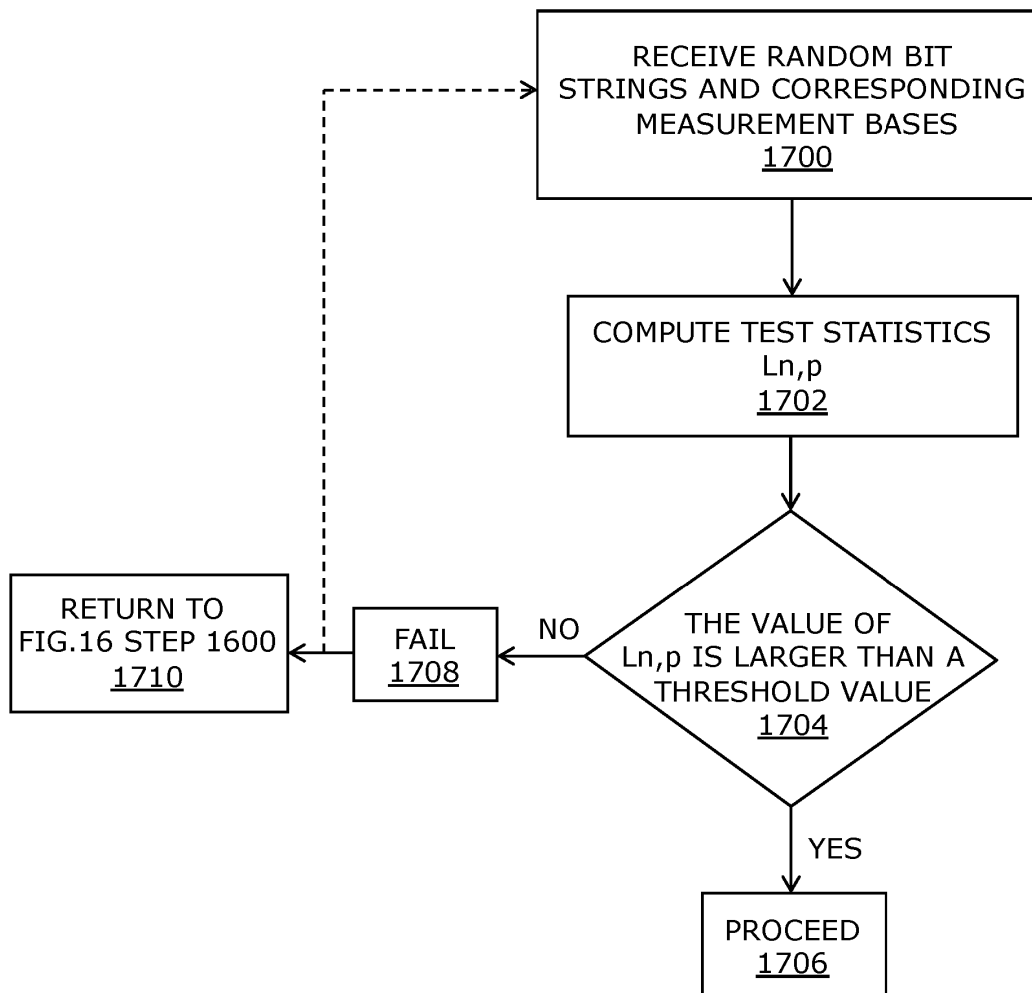
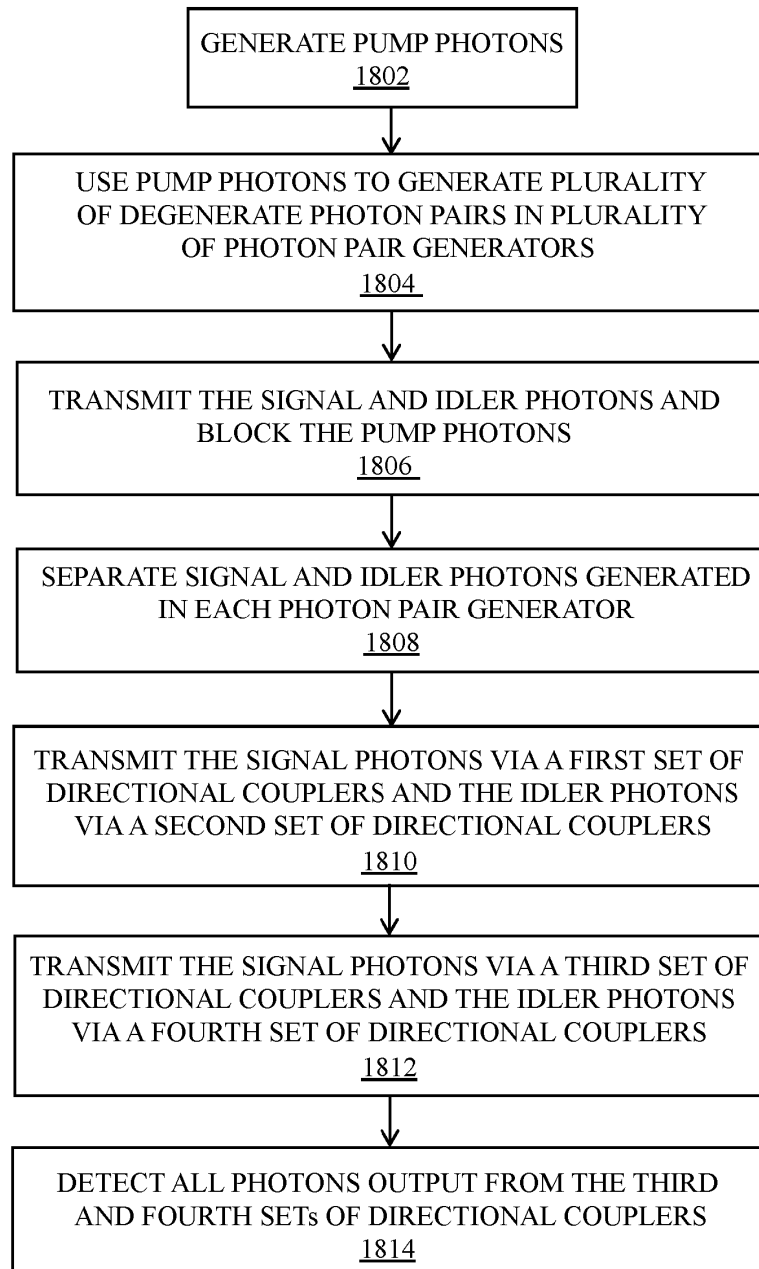
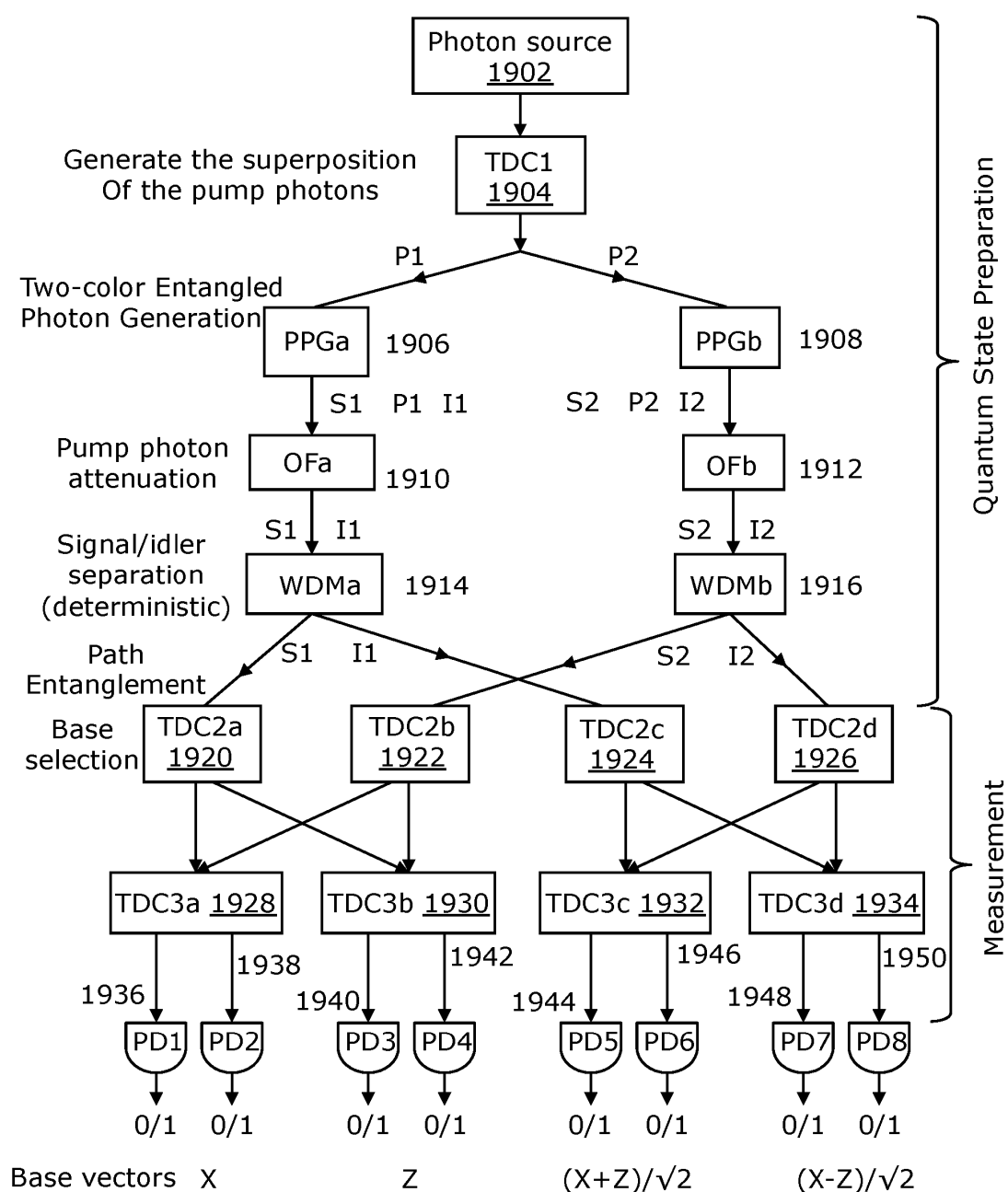


FIG. 15

22/53**FIG. 16**

23/53**FIG. 17**

24/53**FIG. 18**

25/53**FIG. 19**

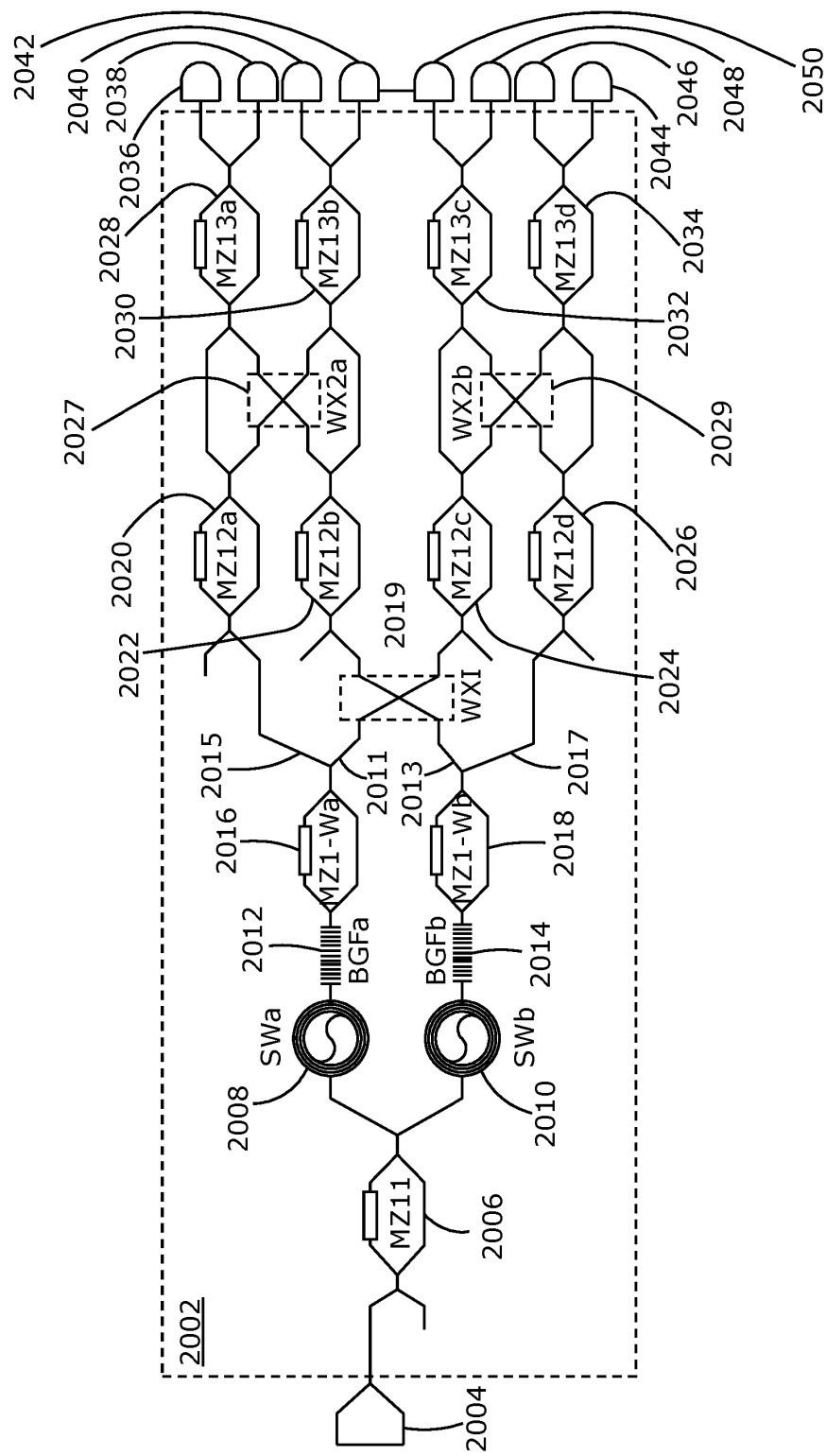


FIG. 20

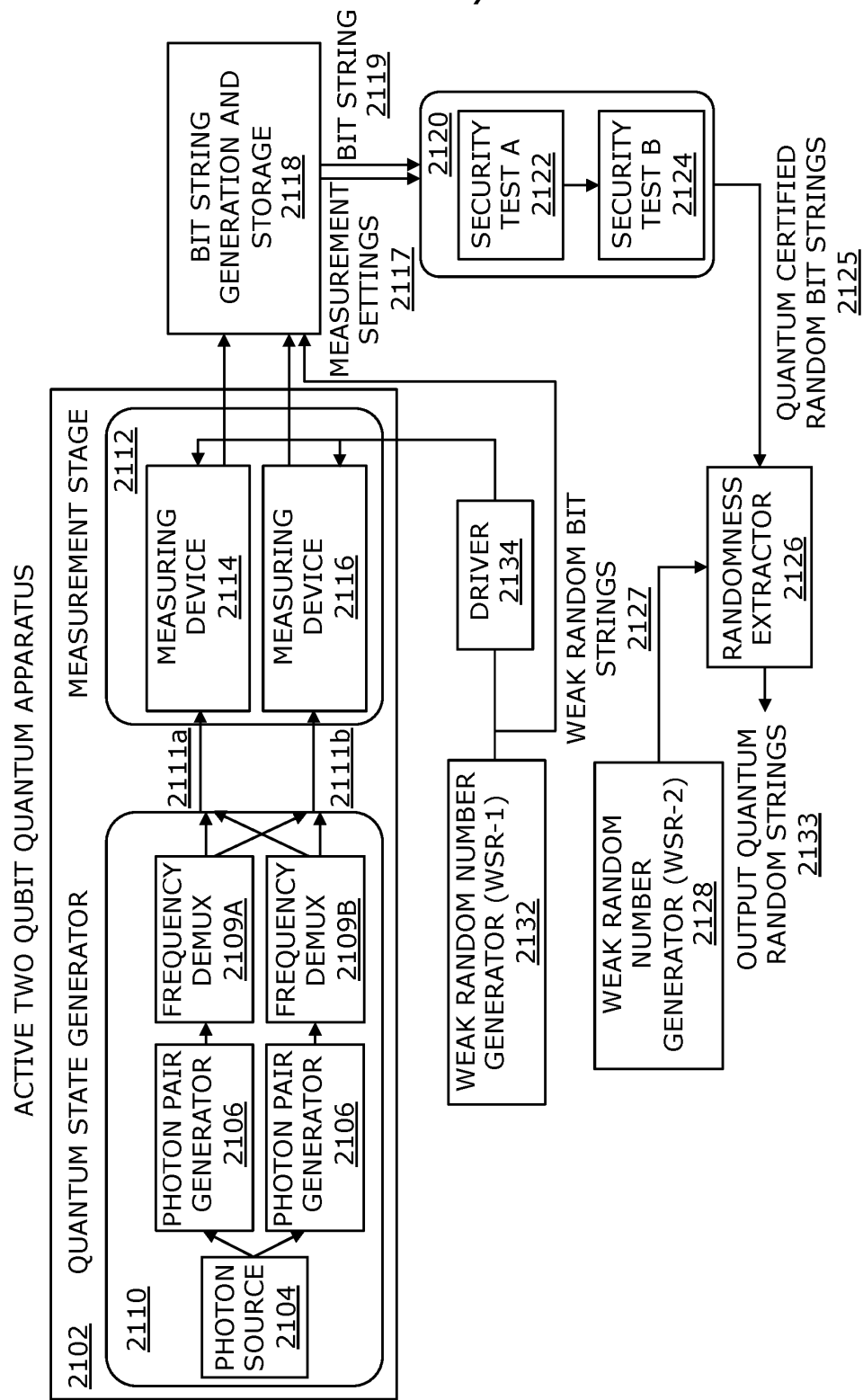
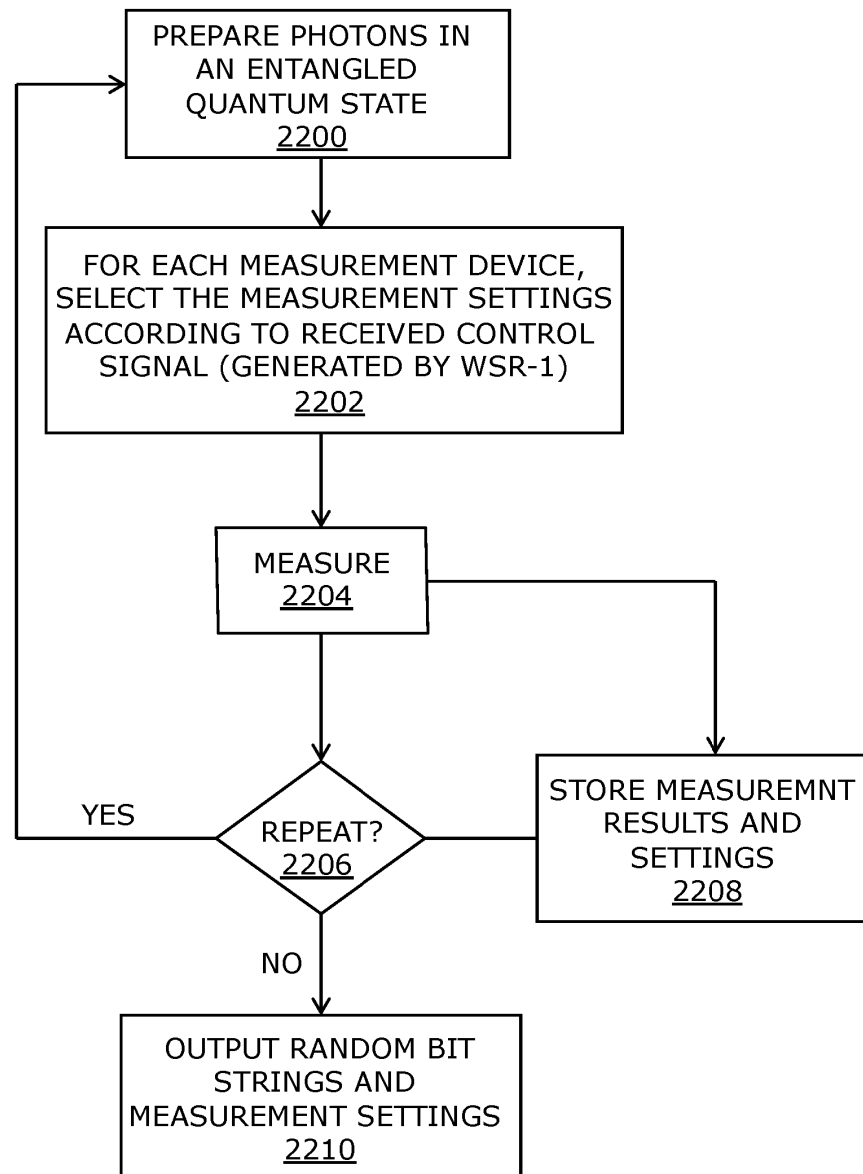
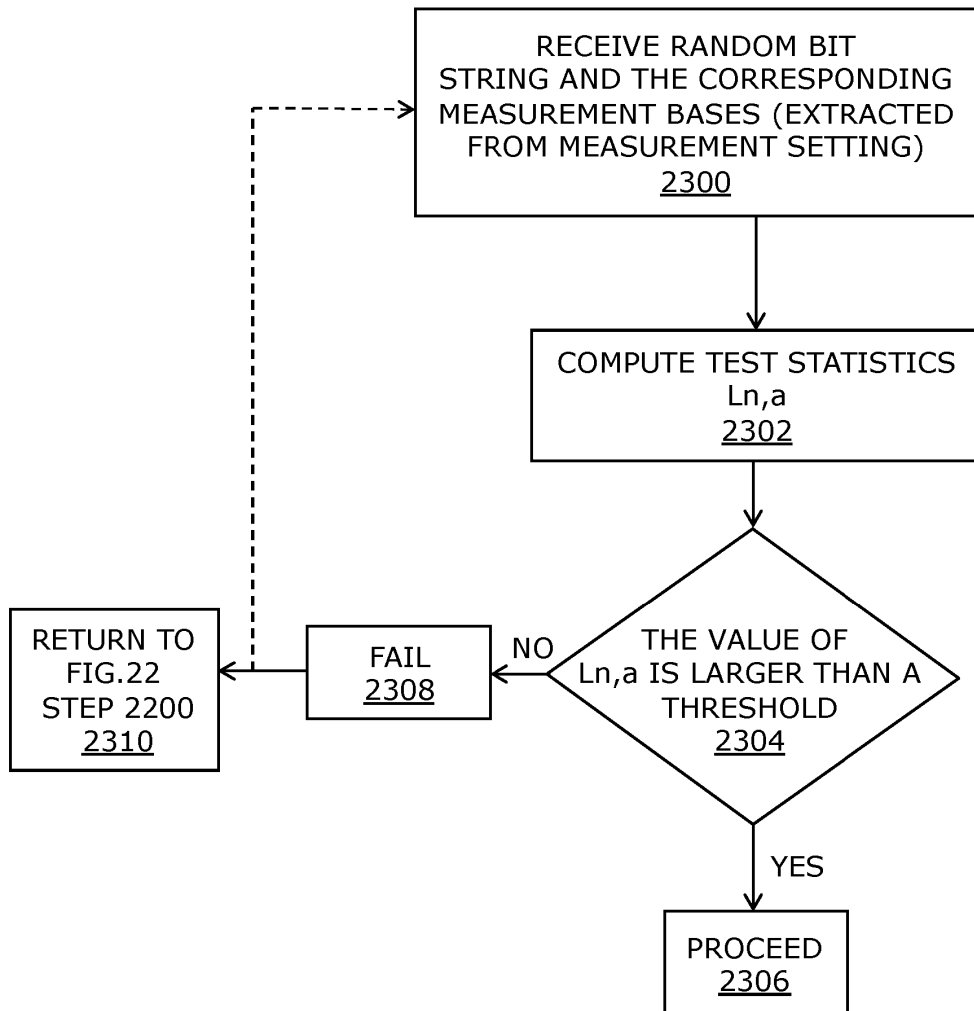
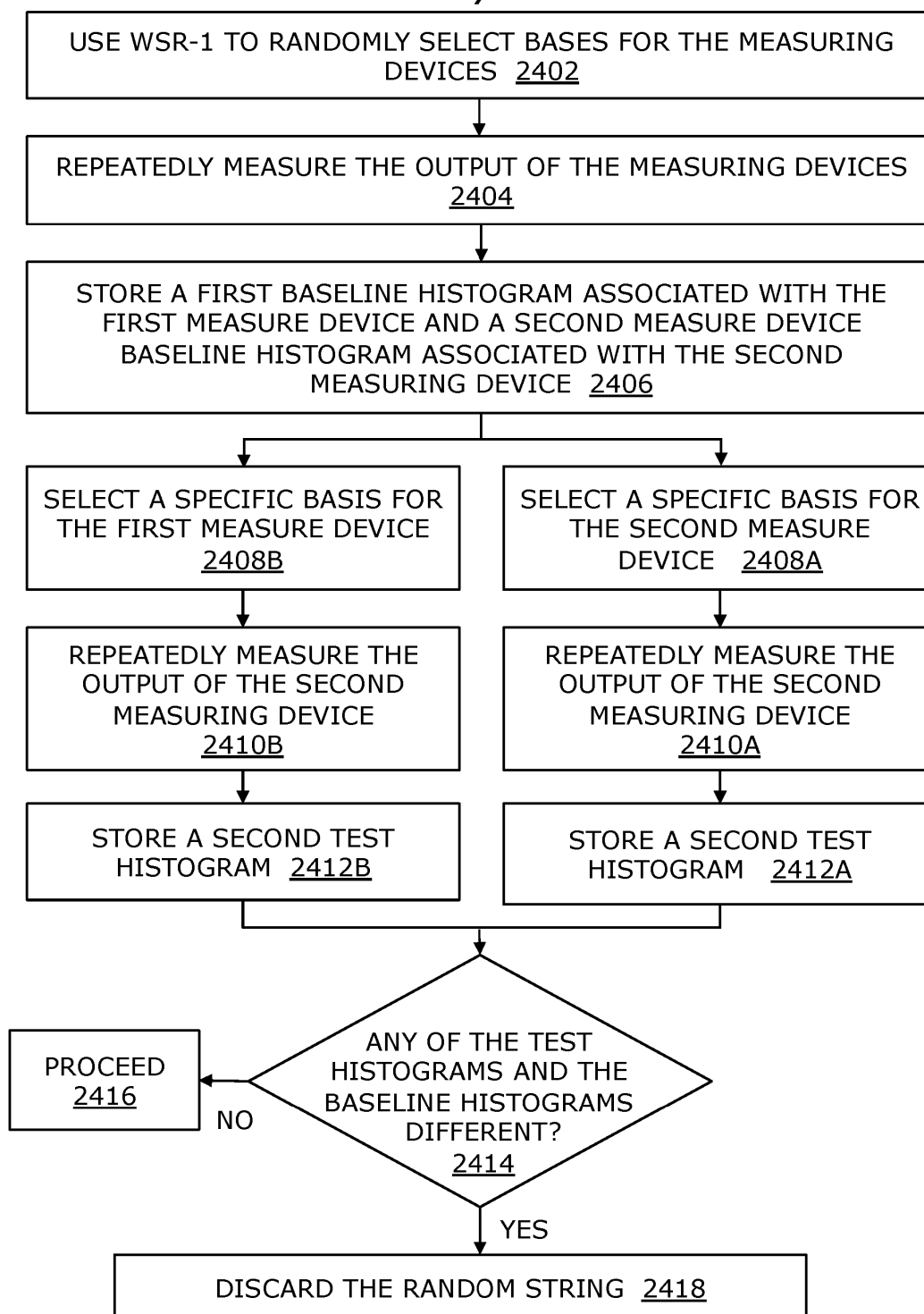
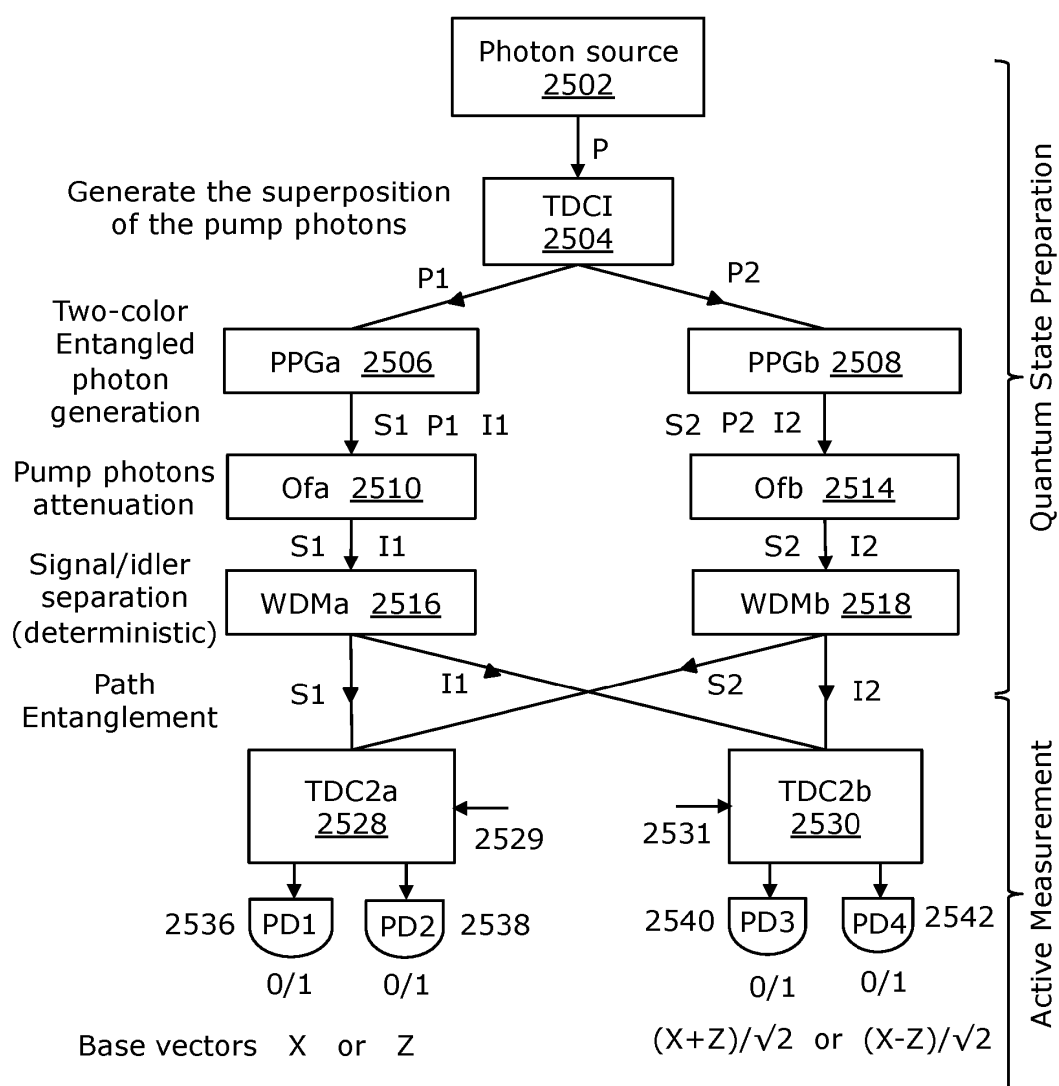


FIG. 21

28/53**FIG. 22**

29/53**FIG. 23**

30/53**FIG. 24**

31/53**FIG. 25**

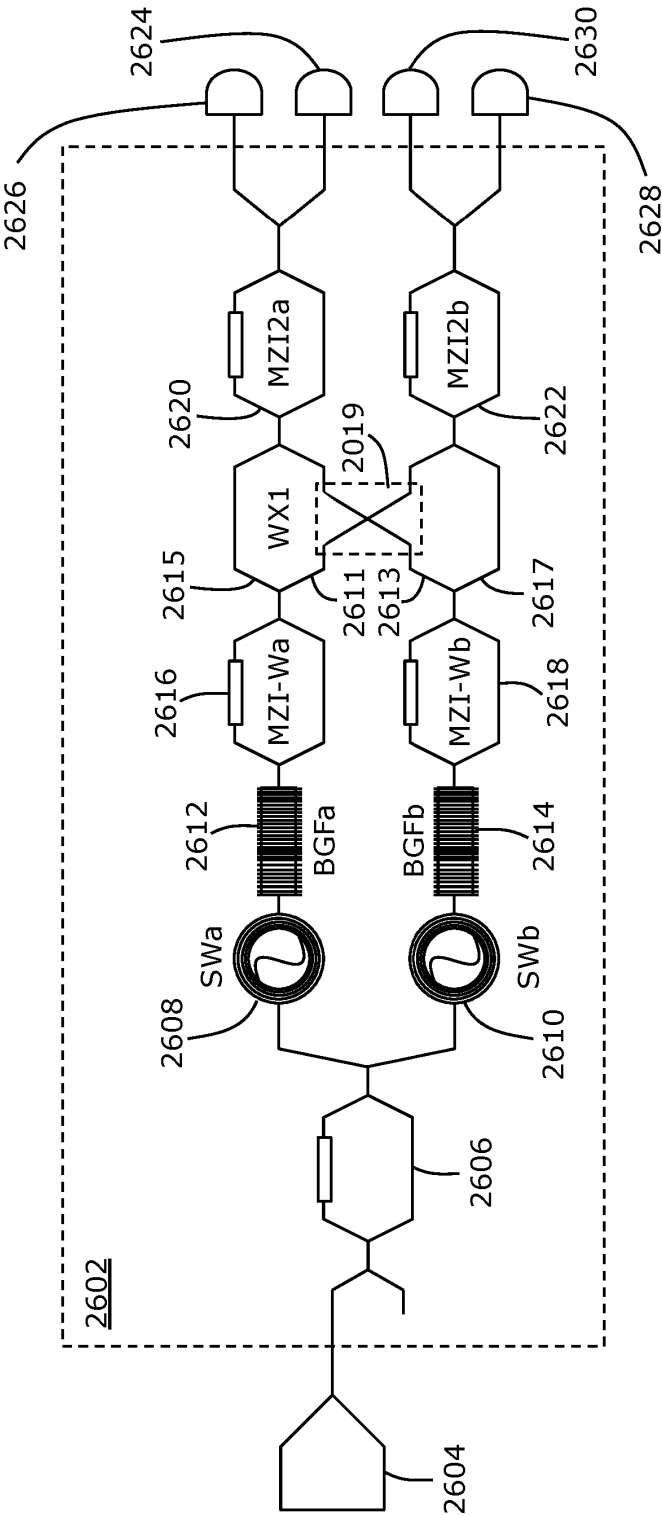


FIG. 26

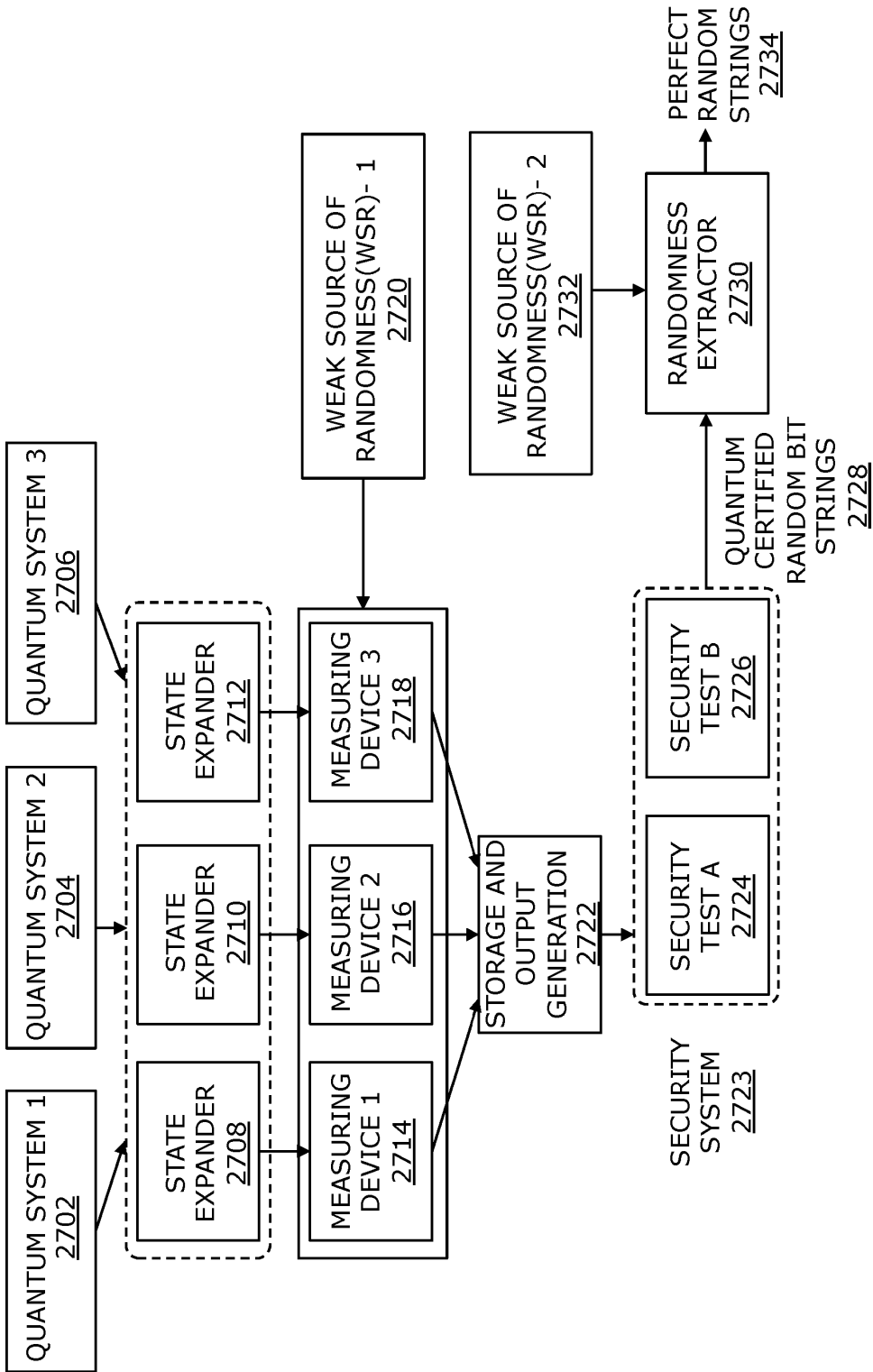


FIG. 27

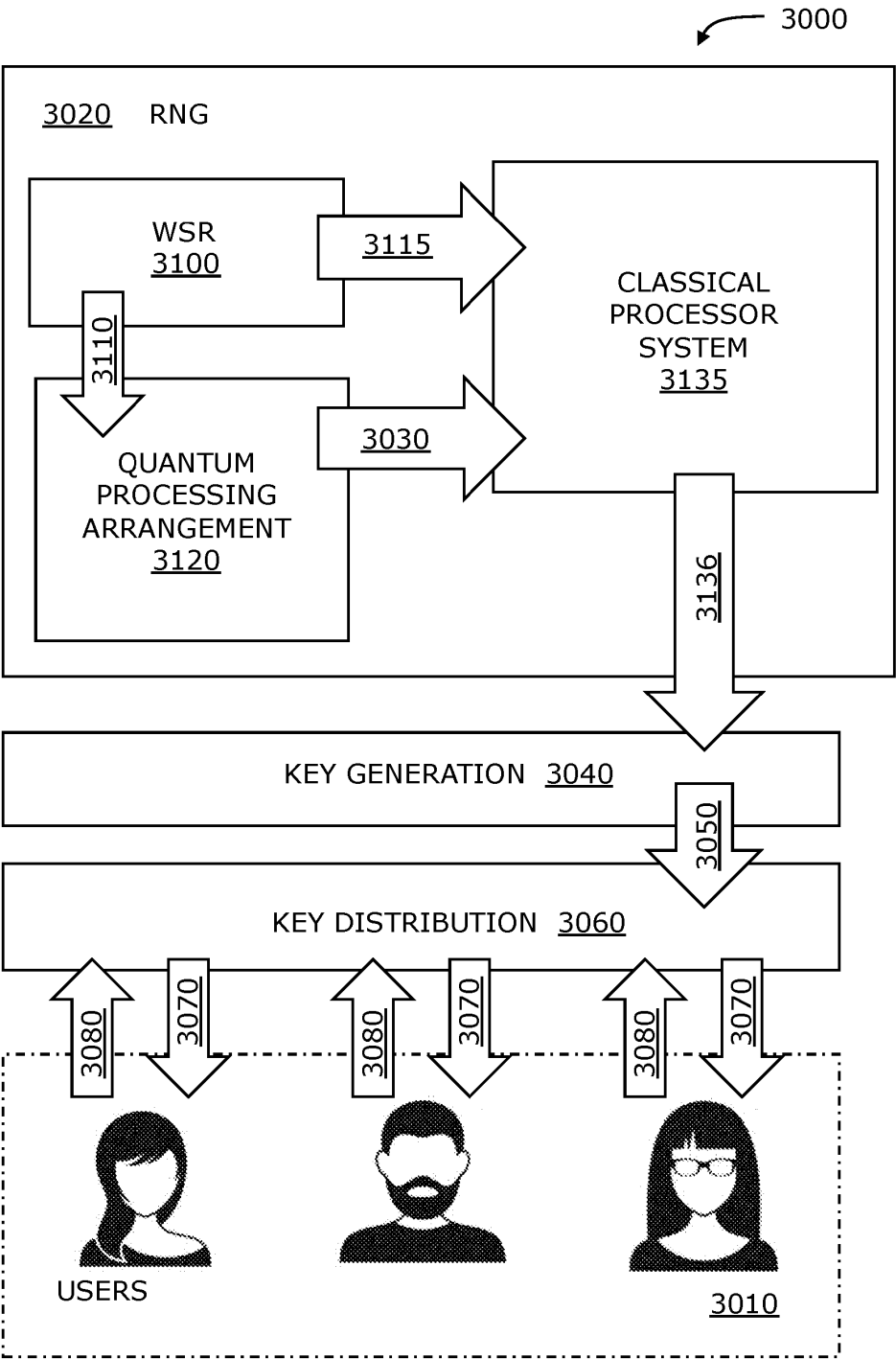


FIG. 28

35/53

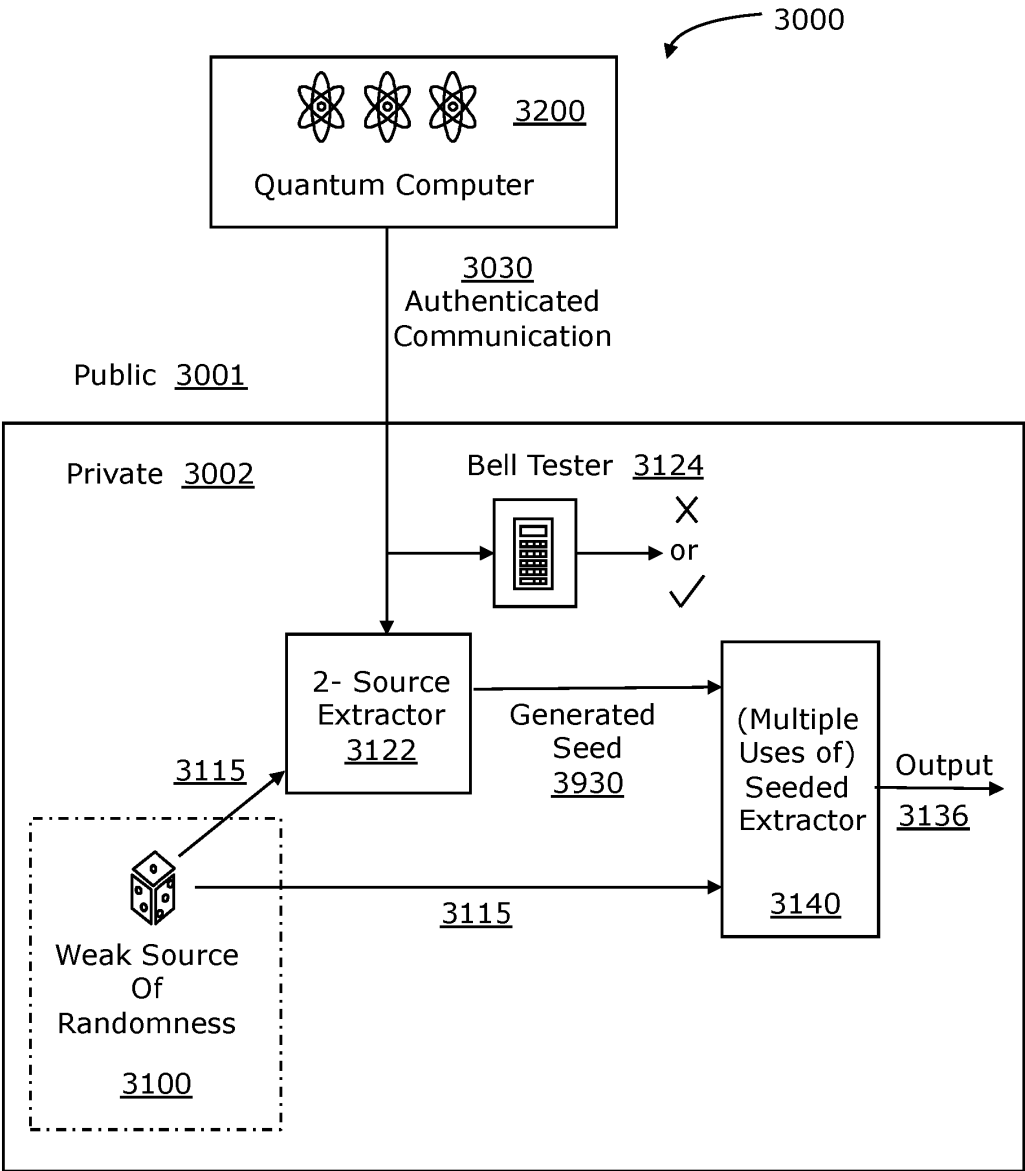
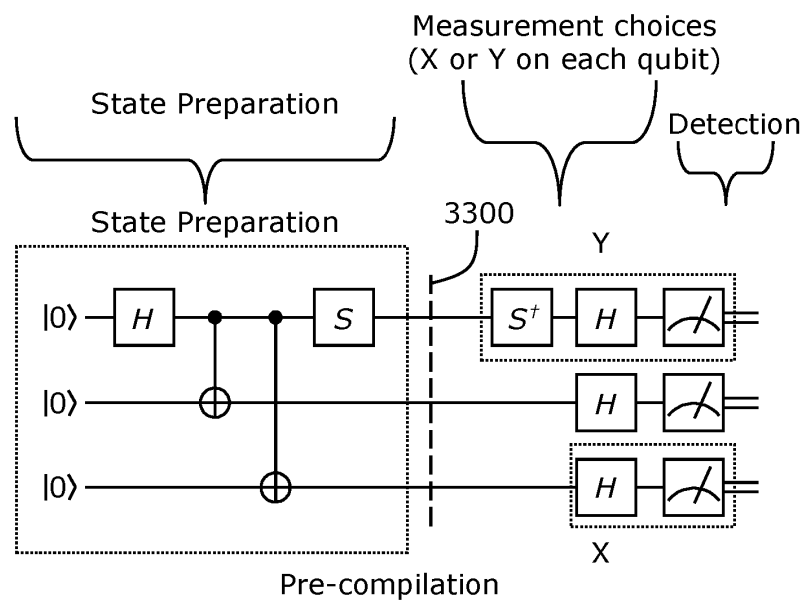
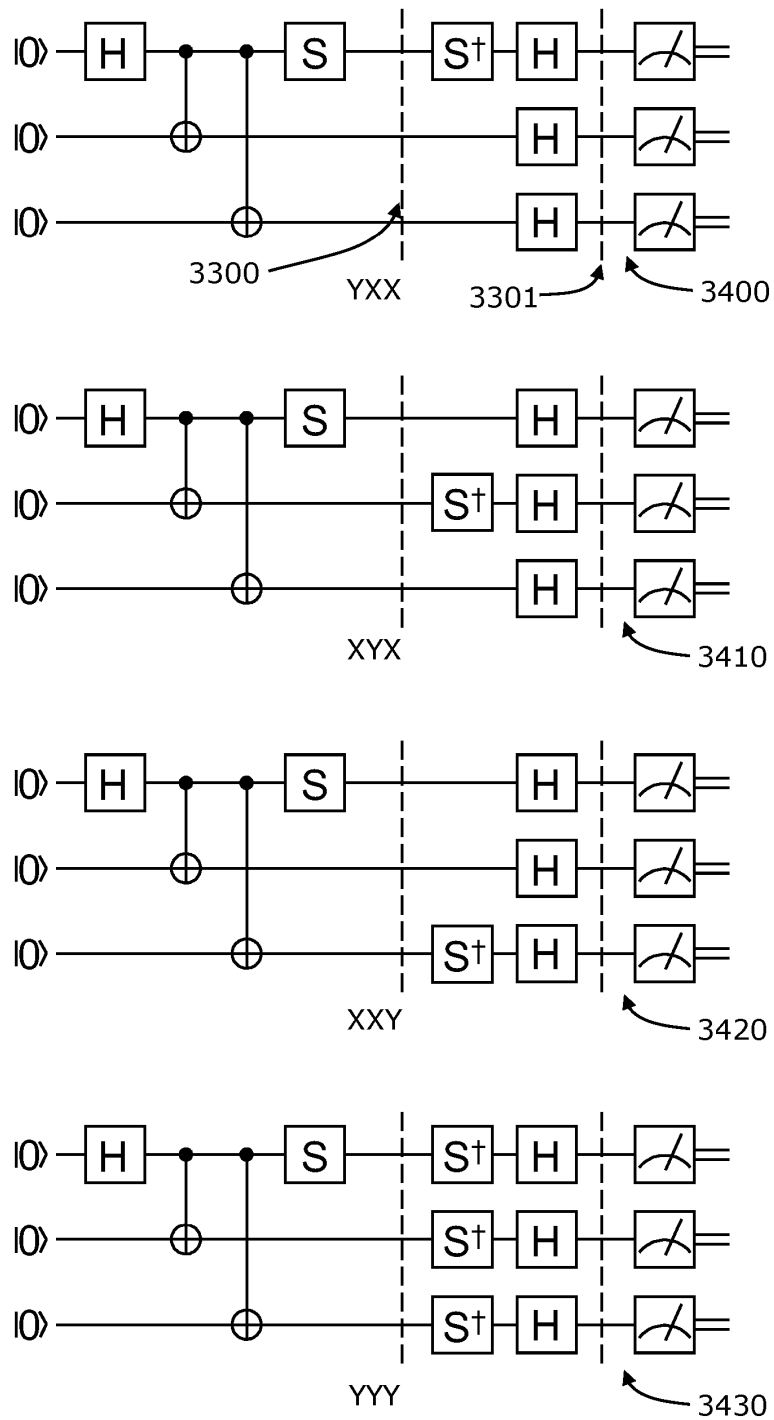


FIG. 29

36/53**FIG. 30**

37/53**FIG. 31**

38/53

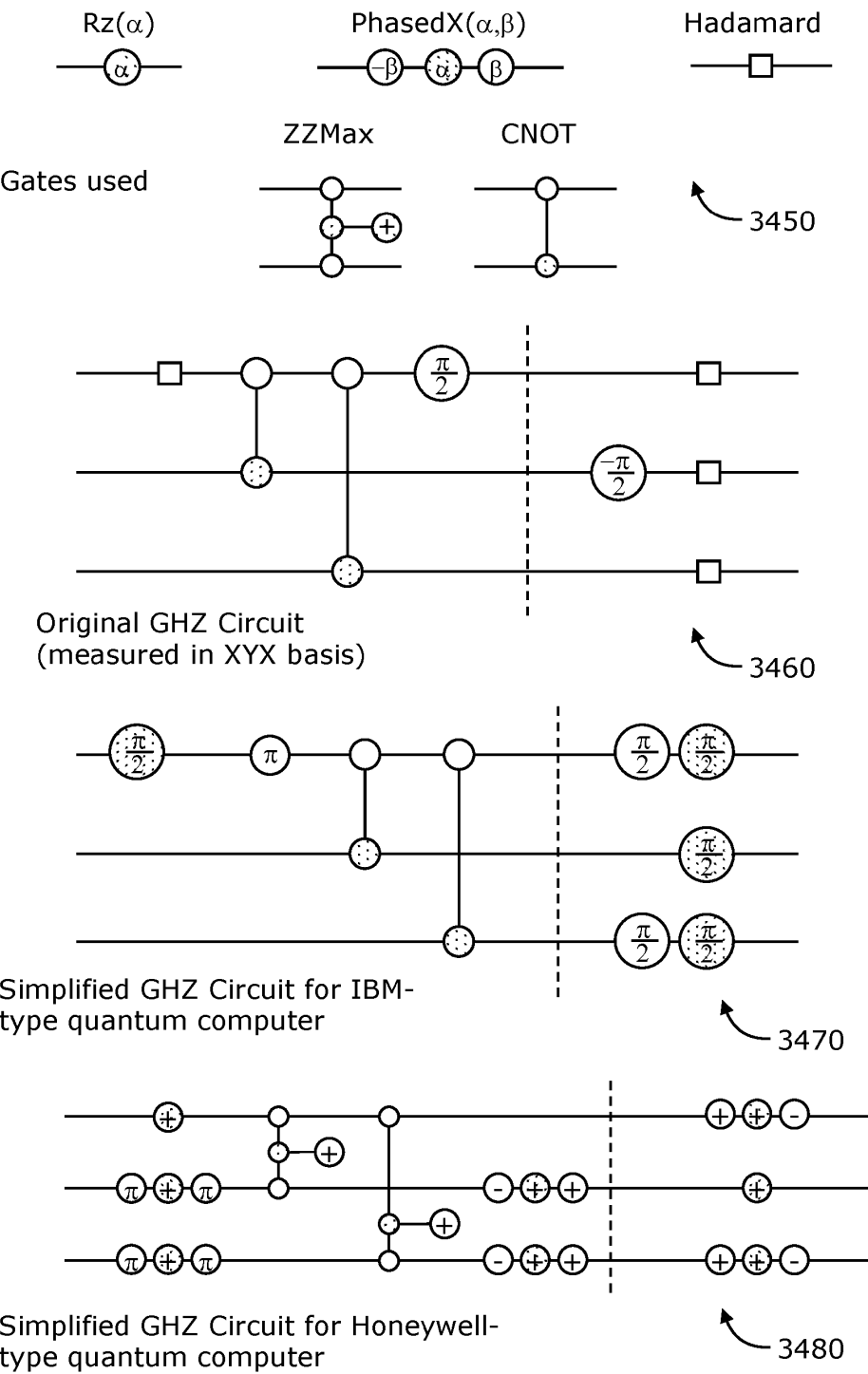


FIG. 32

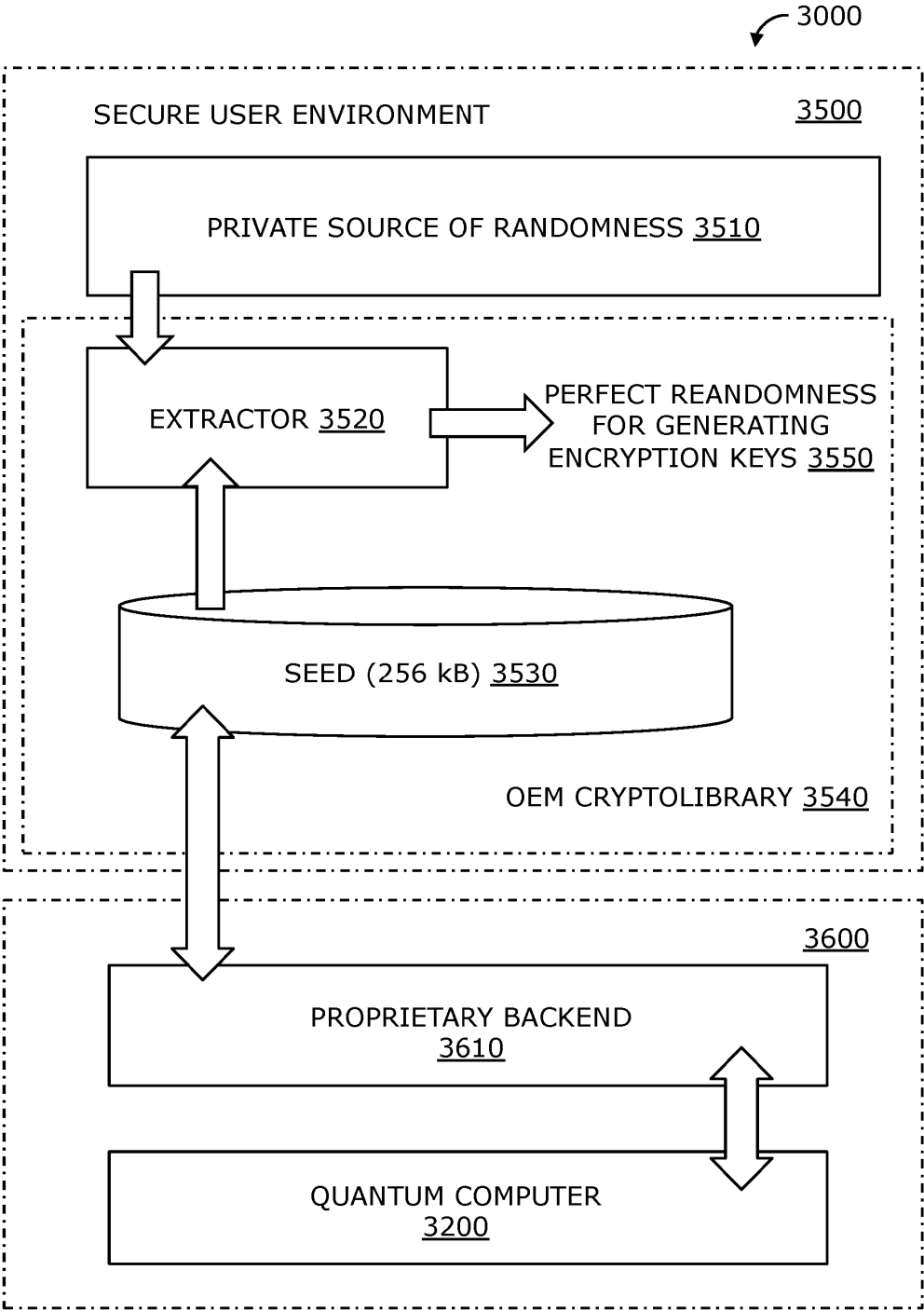


FIG. 33

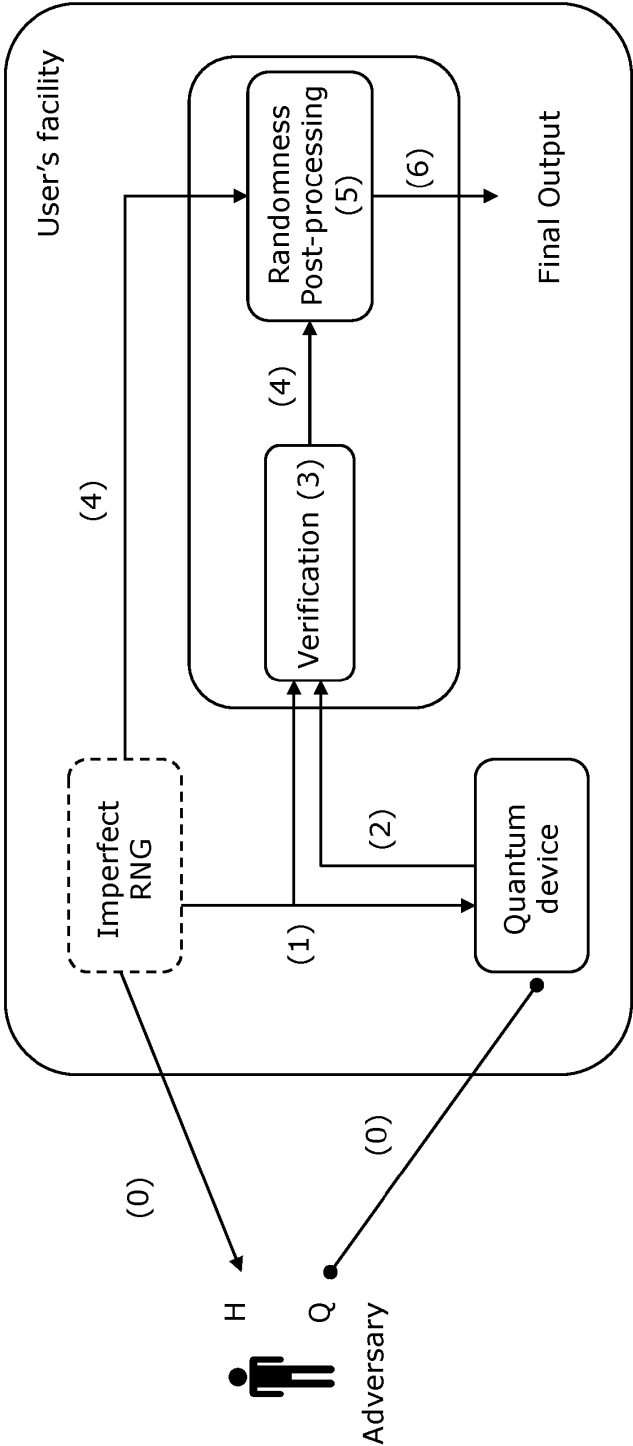


FIG. 34

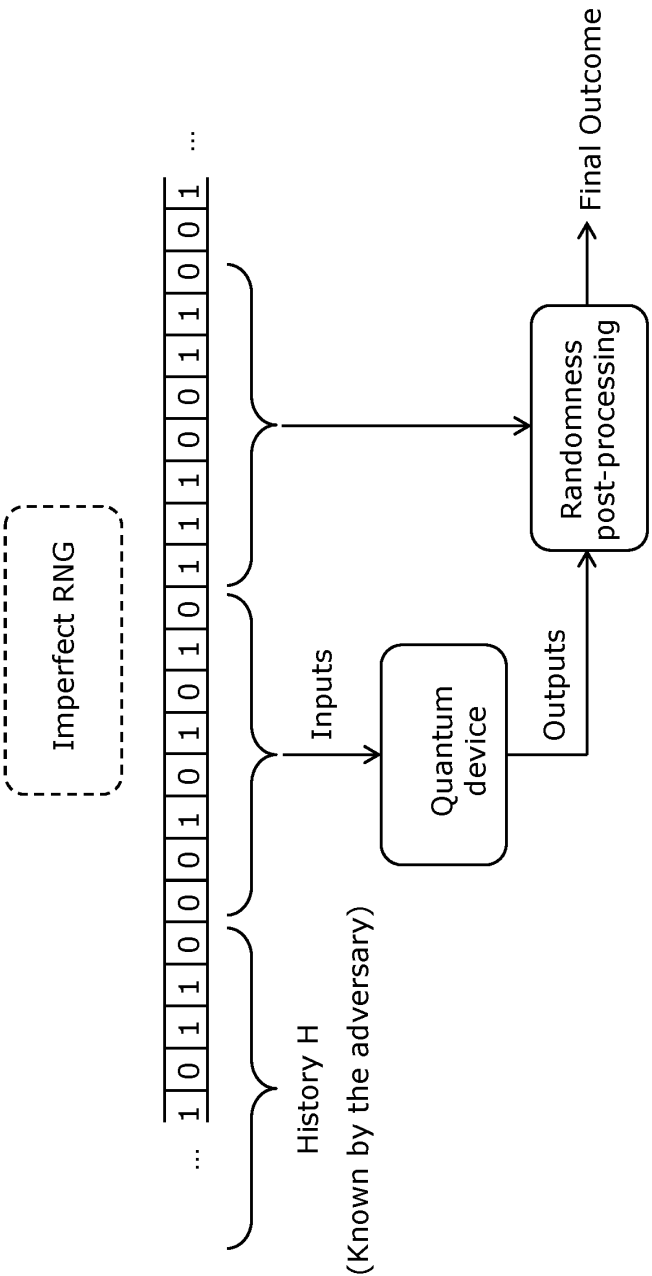


FIG. 35

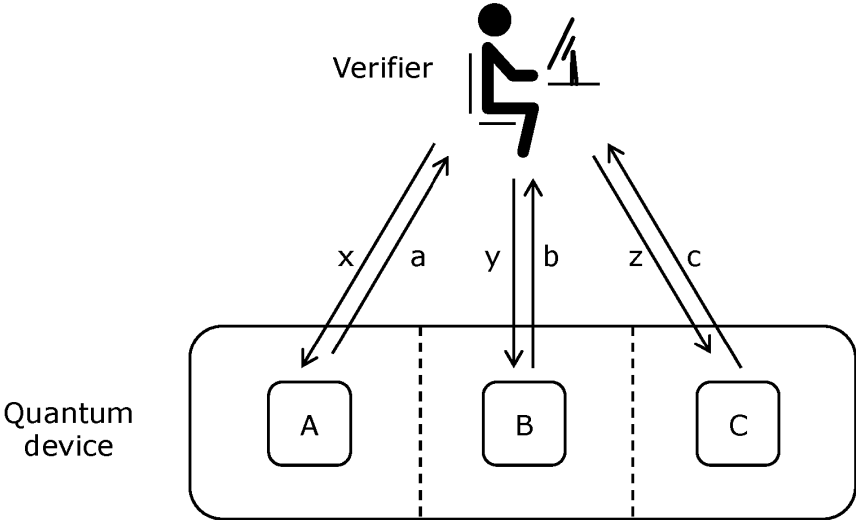
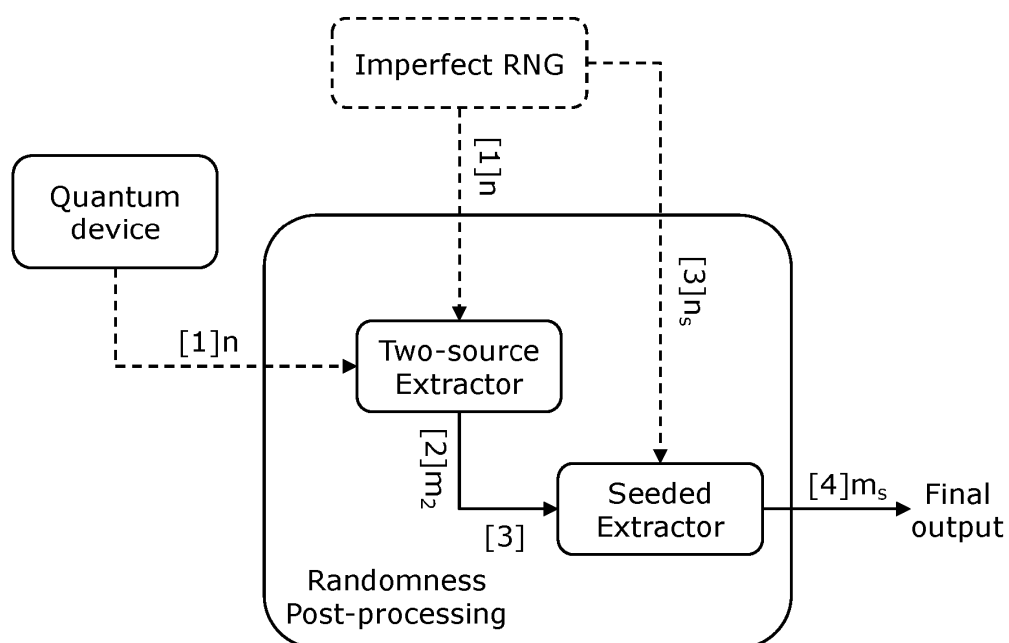
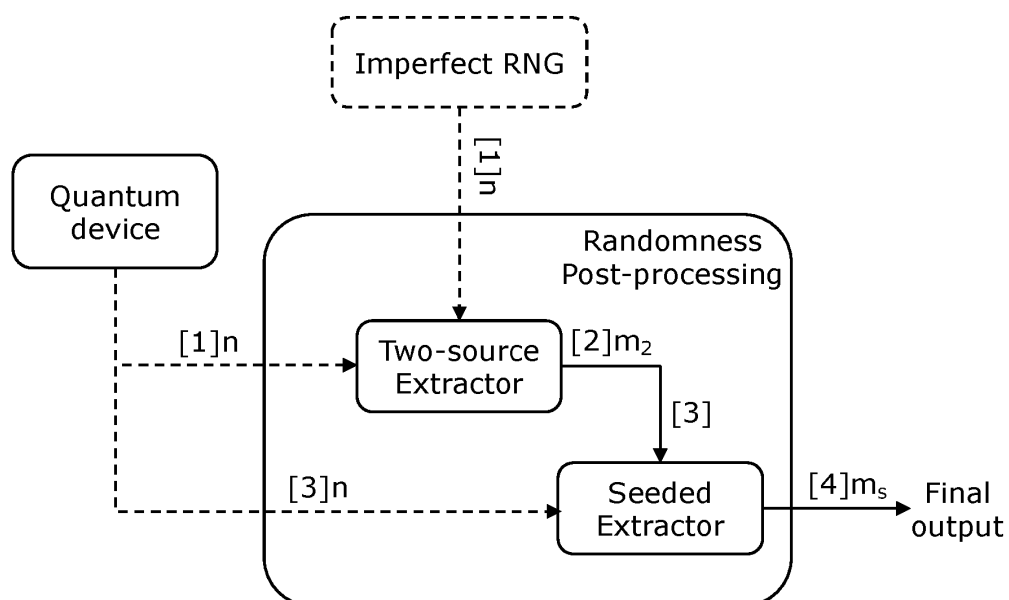


FIG. 36

43/53**FIG. 37****FIG. 38**

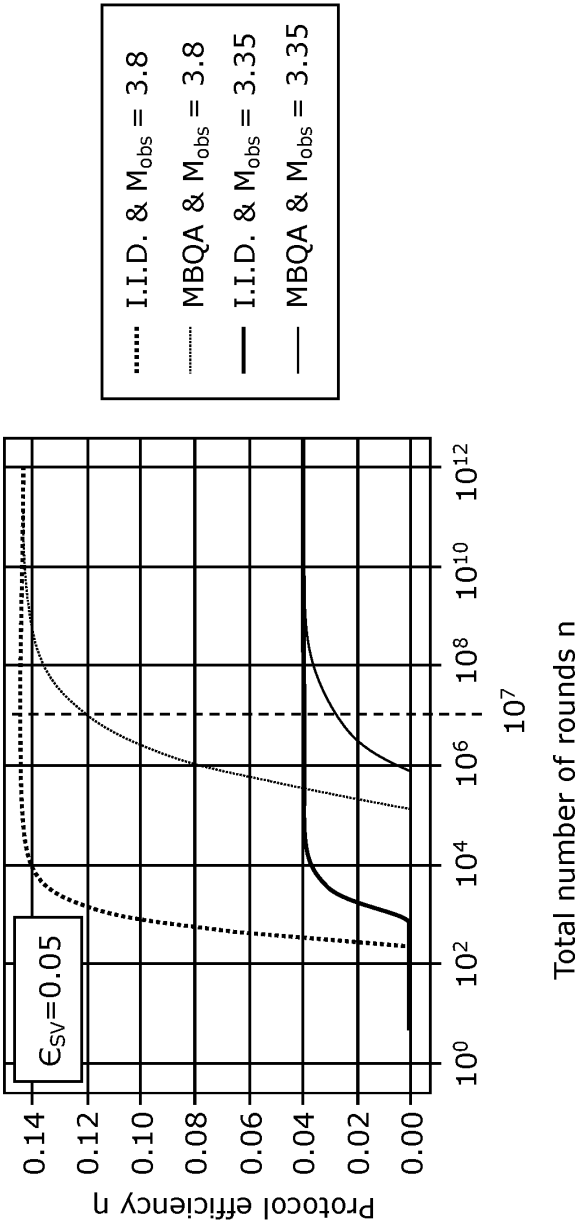


FIG. 39

45/53

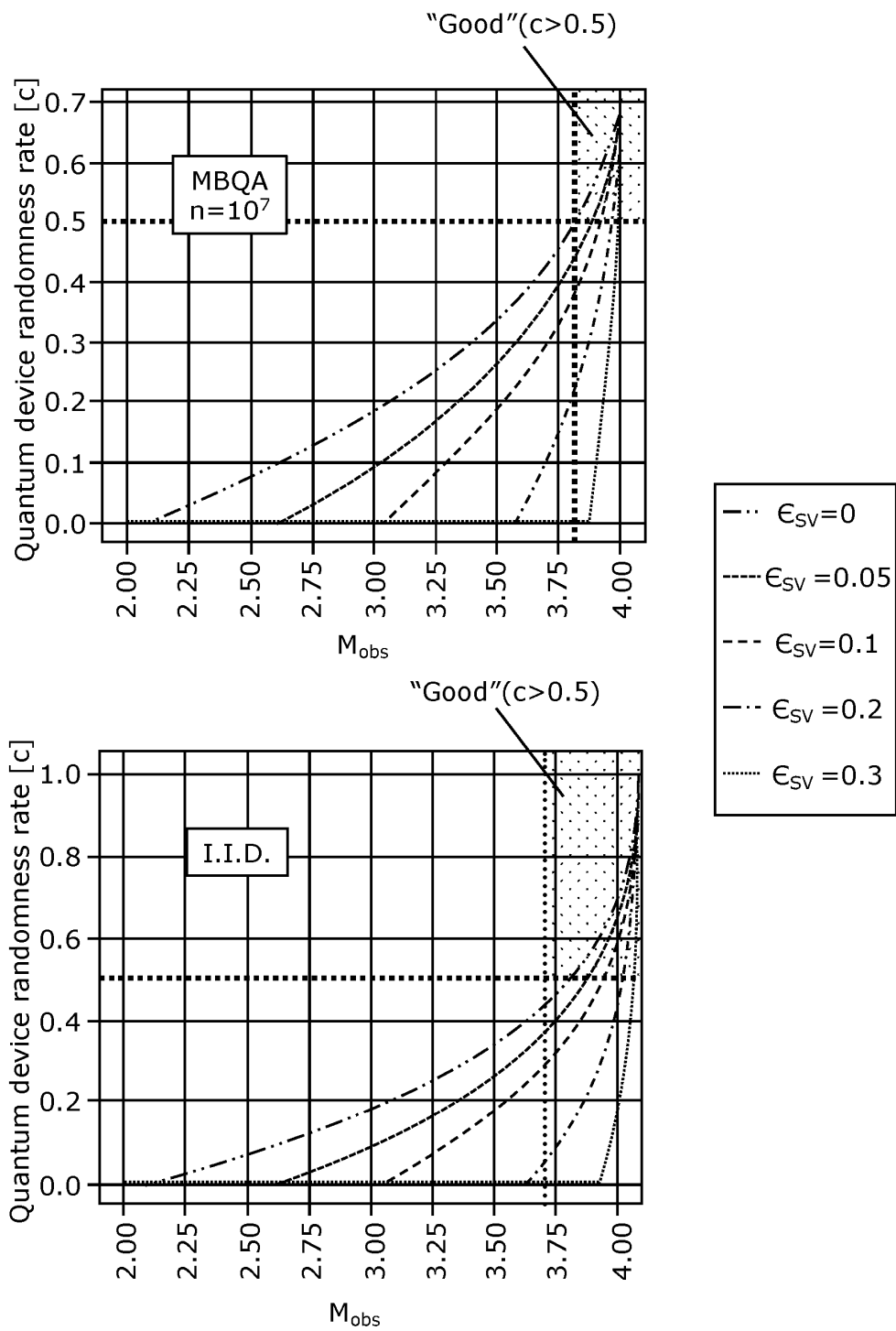


FIG. 40

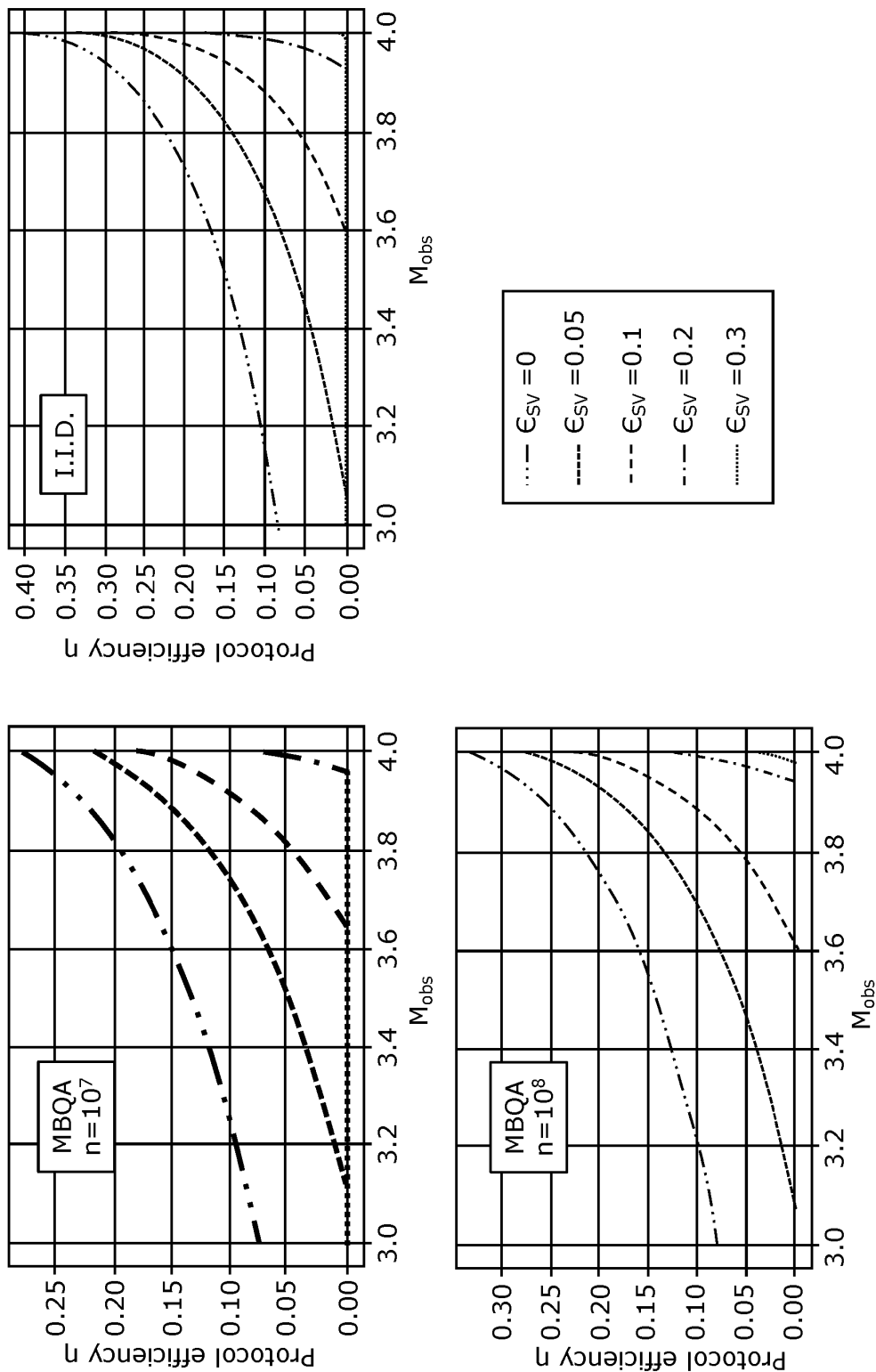


FIG. 41

47/53

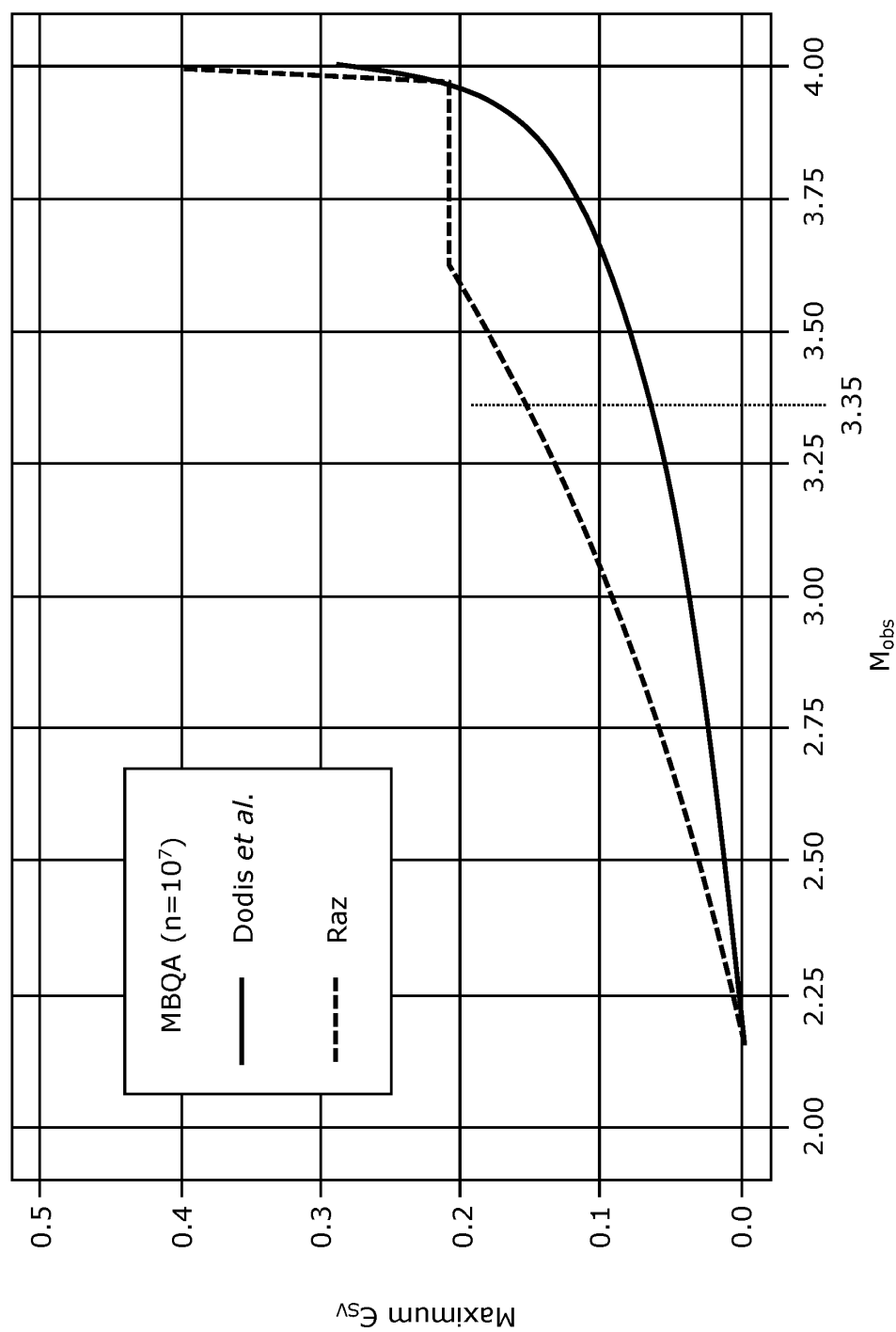


FIG. 42

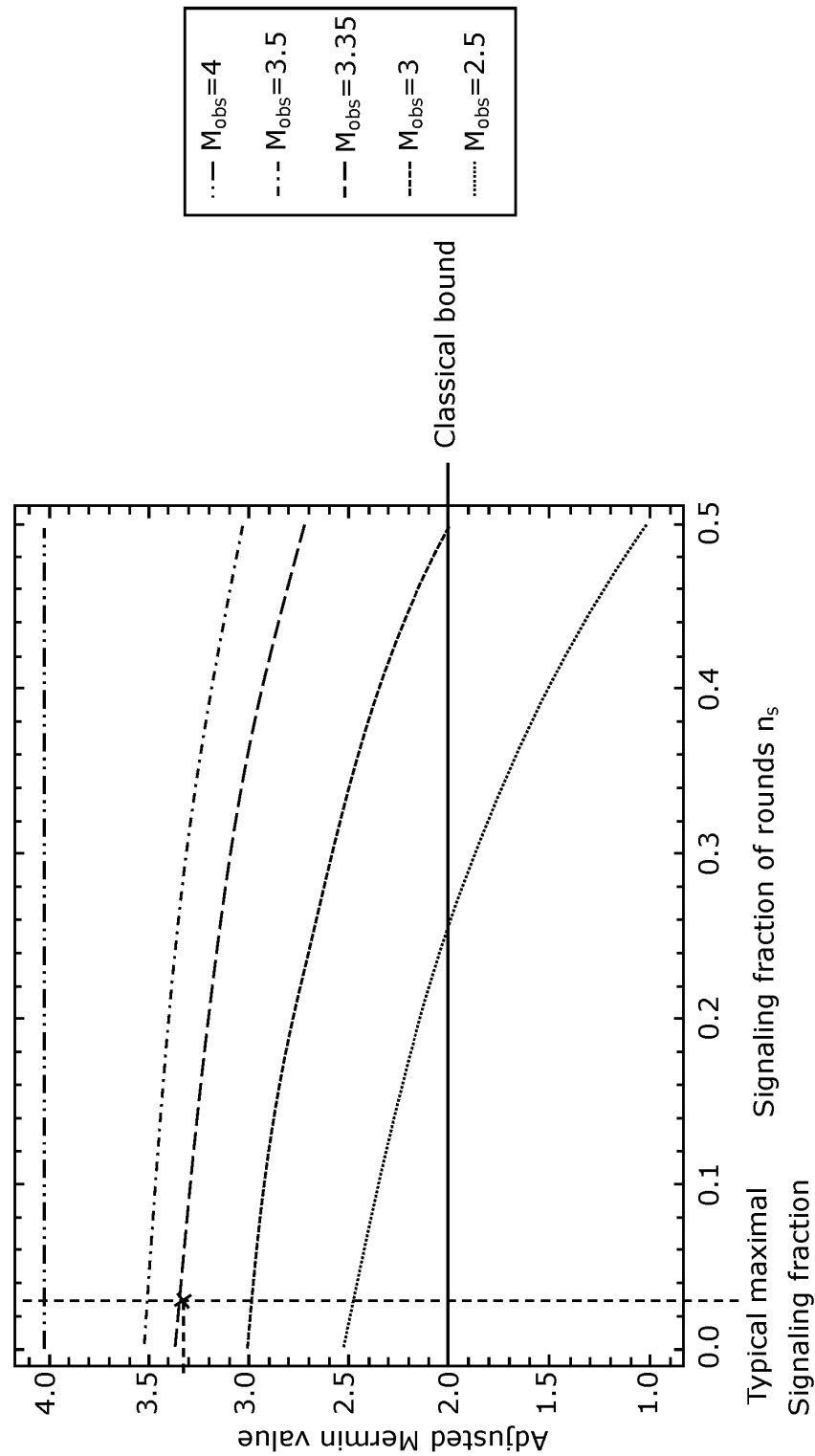


FIG. 43

49/53

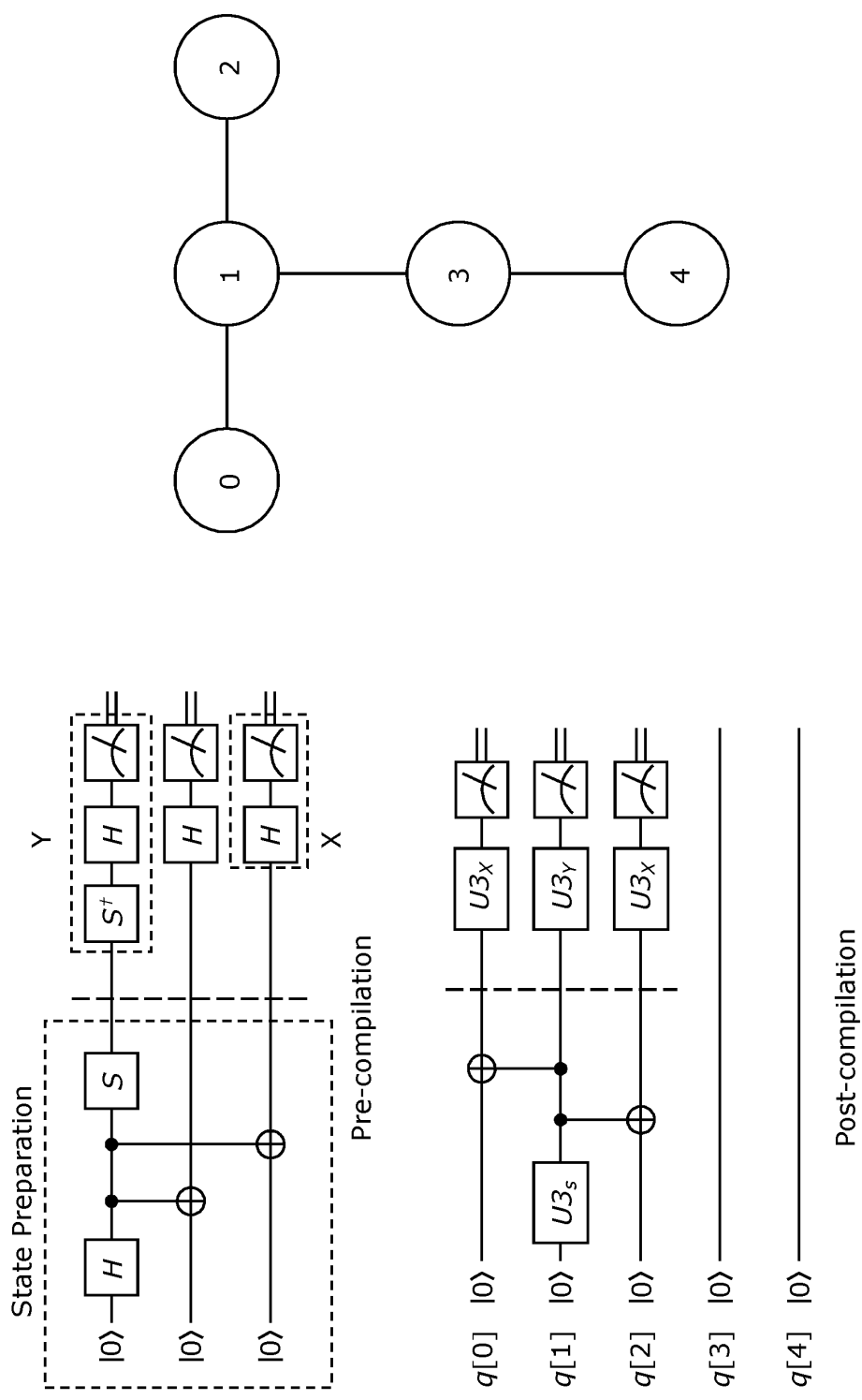


FIG. 44

50/53

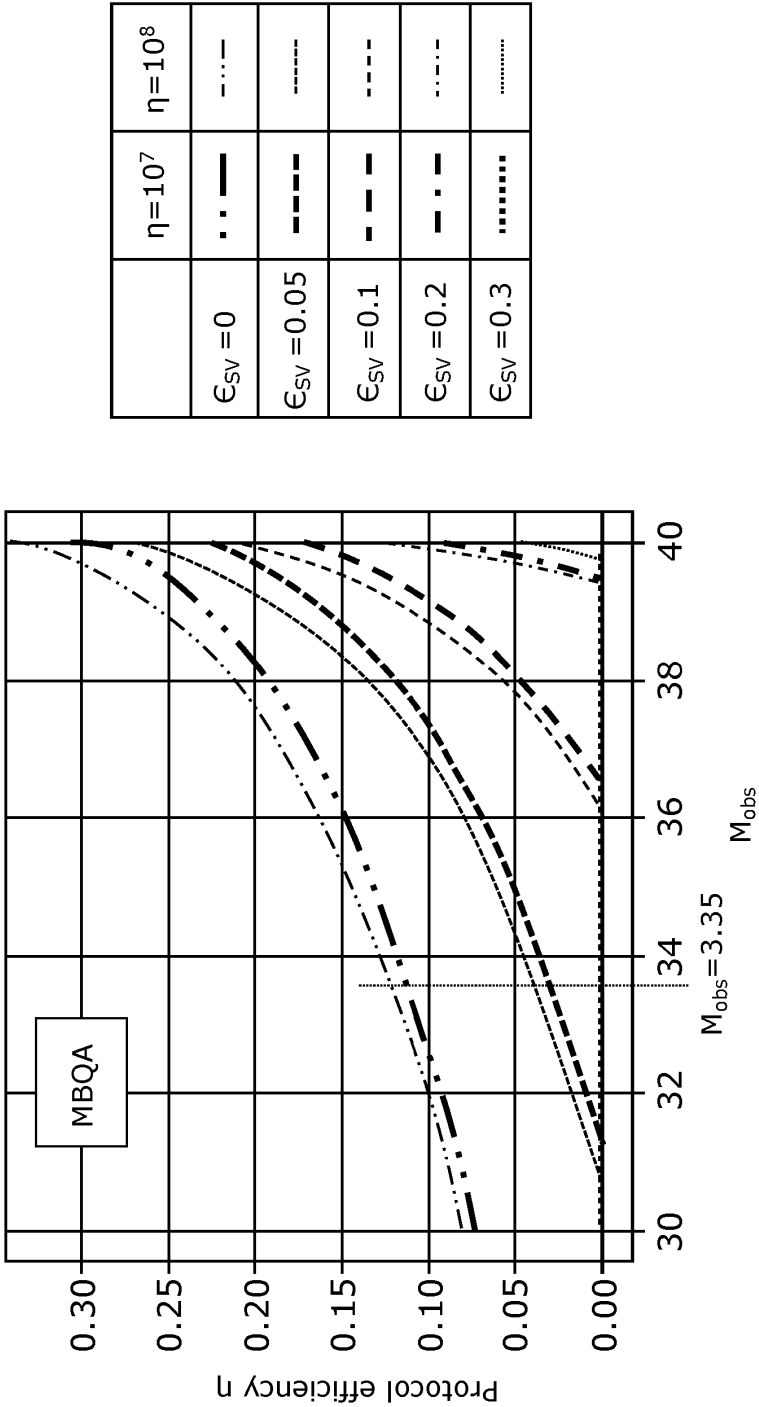


FIG. 45

51/53

- [1] M. Stipcevic and C.K. Koc, "True random number generators," in Open Problems in Mathematics and Computational Science, pp. 275-315, Springer, 2014.
- [2] M. Stipcevic, "Quantum random number generators and their applications in cryptography," in Advanced Photon Counting Techniques VI, vol. 8375, p. 837504, International Society for Optics and Photonics, 2012.
- [3] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Reviews of Modern Physics, vol.89, no.1, p. 015004, 2017.
- [4] M. Santha and U. V. Vazirani, "Generating quasi-random sequences from semi-random sources," Journal of computer and system sciences, vol. 33, no. 1, pp. 75-87, 1986.
- [5] R. Colbeck and R. Renner, "Free randomness can be amplified," Nature Physics, vol. 8, no. 6, pp. 450-153, 2012.
- [6] R. Gallego, L. Masanes, G. De La Torre, C.Dhara, L. Aolita, and A. Acin, "Full randomness from arbitrarily deterministic events," Nature communications, vol. 4, no. 1, pp. 1-7, 2013.
- [7] H. Wojewodka, F.G. Brandao, A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, M. Pawlowski, R. Ramanathan, and M. Stankiewicz, "amplifying the randomness of weak sources correlated with devices," IEEE Transactions on Information Theory, vol. 63, no. 11, pp. 7592-7611, 2017.
- [8] K.-M. Chung, Y. Shi, and X.Wu, "General randomness amplification with non-signaling security," Available: <https://ix.cs.uoregon.edu/xiaodiwu/papers/csw16.pdf>, 2016.
- [9] K.-M. Chung, Y. Shi, and X.Wu, "Physical randomness extractors: generating random numbers with minimal assumptions," arXiv preprint arXiv:1402.4797, 2014.
- [10] F. Brandao, R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, T. Szarek, and H. Wojewodka, "Realistic noise-tolerant randomness amplification using finite number of devices," Nature Communications, vol. 7, no.1, p.11345, 2016.
- [11] R. Ramanathan, F. G. Brandao, K. Horodecki, M. Horodecki, P. Horodecki, and H. Wojewodka, "Randomness amplification against no-signaling adversaries using two devices," arXiv preprint arXiv:1504.06313, 2015.
- [12] R. Ramanathan, M.Horodecki, S.Pironio, K. Horodecki, and P.Horodecki, "Generic randomness amplification schemes using hardy paradoxes," arXiv preprint arXiv:1810.11648, 2018.
- [13] M. Kessler and R. Arnon-Friedman, "Device-independent randomness amplification and privatization," IEEE Journal on Selected Areas in Information Theory, pp. 1-1, 2020.
- [14] A. Acin and L. Masanes, "Certified randomness in quantum physics," Nature, vol. 540, no. 7632, pp. 213-219, 2016.
- [15] C. Foreman, S. Wright, A. Edgington, M. Berta, and F.Curchod, "Practical randomness and privacy amplification: Technical appendices," In preparation, 2020.

FIG. 46A

52/53

- [16] C. Portmann and R. Renner, "Cryptographic security of quantum key distribution," arXiv preprint arXiv:1409.9525, 2014.
- [17] N. D. Mermin, "Extreme quantum entanglement in a superposition of macroscopically distinct states," *Physical Review Letters*, vol. 65, no. 15, p. 1838, 1990.
- [18] E. Woodhead, B. Bourdoncle, and A. Aefn, "Randomness versus nonlocality in the merrin-bell experiment with three parties," *Quantum*, vol. 2, p. 82, 2018.
- [19] F. Dupuis, O. Fawzi, and R. Renner, "Entropy accumulation," arXiv preprint arXiv:1607.01796, 2016.
- [20] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, "Practical device-independent quantum cryptography via entropy accumulation," *Nature communication*, vol. 9, no. 1, pp. 1-11, 2018.
- [21] S. Vadhan, "The unified theory of pseudorandomness: guest column," *SIGACT News*, vol. 38, pp. 39-54, 2007.
- [22] X. Li, "Three-source extractors for polylogarithmic min-entropy," in *Proceedings of the 2015 IEEE 56th Annual Symposium on Foundations of Computer Science (FOCS)*, FOCS '15, (USA), pp. 863-882, IEEE Computer Society, 2015.
- [23] X. Li, "Improved two-source extractors, and affine extractors for polylogarithmic entropy," in *2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 168-177, 2016.
- [24] B. Julsgaard, J. Sherson, J. I. Cirac, J. Fiurasek, and E. S. Polzik, "Experimental demonstration of quantum memory for light," *Nature*, vol. 432, no. 7016, pp. 482-486, 2004.
- [25] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf, "Exponential Separation for one-way Quantum Communication Complexity, with Applications to Cryptography," in *Proc. ACM STOC*, pp. 516-525, ACM Press, 2007.
- [26] R. Arnon-Friedman, C. Portmann, and V. B. Scholz, "Quantum-proof multi-source randomness extractors in the Markov model," in *Proceedings TQC*, vol. 61, pp. 1-34, 2016.
- [27] G. v. Assche, *Quantum cryptography and secret-key distillation*. Cambridge University Press, 2006.
- [28] M. Hayashi and T. Tsurumaru, "More efficient privacy amplification with less random seeds via dual universal hash function," *IEEE Transactions on Information Theory*, vol. 62, no. 4, pp. 2213-2232, 2016.
- [29] Y. Dodis, A. Eibaz, R. Oliveira, and R. Raz, "Improved randomness extraction from two independent sources," in *Proceedings RANDOM*, vol. 3122, pp. 334-344, 2004.
- [30] L. Trevisan, "Extractors and Pseudorandom Generators," *J. ACM*, vol. 48, pp. 860-879, July 2001.
- [31] R. Raz, "Extractors with weak random seeds," in *Proceedings STOC*, pp. 11-20, 2005.
- [32] A. De, C. Portmann, T. Vidick, and R. Renner, "Trevisan's Extractor in the Presence of Quantum Side Information," *SIAM J. Comput.*, vol. 41, pp. 915-940, Jan. 2012.

FIG. 46B

53/53

- [33] W. Maurer, C. Portmann, and V. B. Scholz, "A modular framework for randomness extraction based on Trevisan's construction,"
- [34] M. Berta, O. Fawzi, and V. B. Scholz, "Quantum-proof randomness extractors via operator space theory," *IEEE Transactions on Information Theory*, vol. 63, no. 4, pp. 2480-2503, 2016.
- [35] Y.-A. Chen, T. Yang, A.-N. Zhang, Z. Zhao, A. Cabello, and J.-W. Pan, "Experimental violation of Bell's inequality beyond tsirelson's bound," *Physical review letters*, vol. 97, no. 17, p. 170408, 2006.
- [36] D.M. Greenberger, M. A. Horne, and A. Zeilinger, "Going beyond Bell's theorem," in *Bell's theorem, quantum theory and conceptions of the universe*, pp. 69 -72. Springer, 1989.
- [37] S. Sivarajah, S. Dilkes, A. Cowtan, W. Simmons, A. Edgington and R. Duncan. " $|t\rangle$: A retargetable compiler for NISQ devices," *Quantum Science and Technology*, 2020.
- [38] D. Gonzalez, D.F. de la Pradilla, and G.Gonzalez, "Revisiting the experimental test of Mermin's inequalities at IBMQ," *arXiv preprint arXiv:2005.11271*, 2020.
- [39] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker. "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *tech. rep., Booz-allen and hamilton inc mclean va*, 2001.

FIG. 46C