CLAIMS

1. A system for randomness extraction for quantum cryptography, comprising

a sampling module configured to sample a cryptographic key to generate one or more sub-blocks;

an entropy module configured to determine a lower bound of the entropy in each sub-block, wherein the determining of the lower bound comprises consideration of correlations between each sub-block and unsampled bits of the cryptographic key and/or other sub-blocks; and

a hashing module configured to hash each sub-block for randomness extraction on each sub-block.

2. The system of claim 1, wherein the cryptographic key comprises either a raw key or a sifted key.

3. The system of claims 1 or 2, wherein the sampling module is configured to sample the cryptographic key into the one or more sampled sub-blocks in a random manner based on a pre-determined probability.

4. The system of any one of the preceding claims, comprising a sifting module configured to sift the cryptographic key or to sift the one or more sampled sub-blocks.

5. The system of any one of the preceding claims, wherein the sampling module is configured to apply a thresholding on the length of bit strings representing the respective sub-blocks and to abort the method if the length of the bit string for any sub-block exceeds a predetermined threshold.

6. The system of any one of the preceding claims, comprising a concatenation module configured to concatenate the hashed sub-blocks to generate a secret key.

7. The system of any one of the preceding claims, wherein the entropy module is configured to determine the lower bound based on the generalized entropy-accumulation theorem.

8. A method of randomness extraction for quantum cryptography, comprising the steps of:

sampling a cryptographic key to generate one or more sub-blocks;

determining a lower bound of the entropy in each sub-block, wherein the determining of the lower bound comprises consideration of correlations between each sub-block and unsampled bits of the cryptographic key and/or other sub-blocks; and

hashing each sub-block for randomness extraction on each sub-block.

9. The method according to claim 8, wherein the cryptographic key comprises either a raw key or a sifted key.

10. The method according to claims 8 or 9, wherein the step of sampling the raw key into the one or more sub-blocks is performed in a random manner based on a pre-determined probability.

11. The method of any one of claims 8 to 10, comprising sifting the cryptographic key or sifting the one or more sampled sub-blocks.

12. The method of any one of claims 8 to 11, comprising applying a thresholding on the length of bit strings representing the respective sub-blocks and aborting the method if the length of the bit string for any sub-block exceeds a predetermined threshold.

13. The method of any one of claims 8 to 12, comprising concatenating the hashed sub-blocks to generate a secret key.

14. The method of any one of claims 8 to 13, wherein the step of determining the lower bound is based on the generalized entropy-accumulation theorem.

15. A method of performing quantum cryptography between two or more parties, the method comprising:

sampling a cryptographic key to generate one or more sub-blocks;

announcing a uniform random variable $V_i \in [1, N_S]$, wherein N_S is equal to the number of sub-blocks and i identifies a bit number of the cryptographic key such that $V_i$identifies which bit of the cryptographic key is sampled into which sub-block;

wherein the method uses the system for randomness extraction for quantum cryptography of any one of claims 1 to 7.

16. A method of performing quantum cryptography between two or more parties, the method comprising:

sampling a cryptographic key to generate one or more sub-blocks;

announcing a uniform random variable $V_i \in [1, N_S]$, wherein N_S is equal to the number of sub-blocks and i identifies a bit number of the cryptographic key such that $V_i$identifies which bit of the cryptographic key is sampled into which sub-block;

wherein the method comprises using the method for randomness extraction for quantum cryptography of any one of claims 8 to 14.