CLAIMS

1. A measurement-device-independent (MDI) quantum key distribution (QKD) network comprising:

a common server with a laser source for optical pulse generation and distribution;

a plurality of user systems, each user system configured to:

receive the optical pulses from the common server;

modulate the optical pulses for quantum communication; and

re-transmit the modulated optical pulses to the common server;

wherein each user system comprises an energy bounding component for limiting Trojan horse attack (THA); and

wherein the energy bounding component comprises a power limiter limiting the re-transmitted modulated optical pulses to a maximum intensity during a THA.

2. The MDI QKD network of claim 1, wherein the common server comprises one or more detectors for generating measurement results from the re-transmitted modulated optical pulses from a pair of user systems.

3. The MDI QKD network of claim 2, wherein the common server comprises one or more time delay modules for timing calibration of the re-transmitted modulated optical pulses from the pair of user systems.

4. The MDI QKD network of claims 2 or 3, comprising a classical communication channel between the common server and each of the user systems for communicating the measurement results.

5. A method of operating a measurement-device-independent (MDI) quantum key distribution (QKD) network comprising a common server and a plurality of user systems, the method comprising the steps of:

performing optical pulse generation and distribution using a laser source at the common server;

receiving the optical pulses at the user systems from the common server;

modulating the optical pulses at the user systems for quantum communication;

re-transmitting the modulated optical pulses from the user systems to the common server; and

using an energy bounding component at each of the user system for limiting Trojan horse attack (THA);

wherein the energy bounding component comprises a power limiter and limiting the THA comprises using the power limiter for limiting the re-transmitted modulated optical pulses to a maximum intensity during a THA.

6. The method of claim 5, comprising generating measurement results from the re-transmitted modulated optical pulses from a pair of user systems received at the common server.

7. The method of claim 6, comprising using one or more time delay modules for timing calibration of the re-transmitted modulated optical pulses from the pair of user systems at the common server.

8. The method of claims 6 or 7, comprising using a classical communication channel between the common server and each of the user systems for communicating the measurement results.

9. A user system for a measurement-device-independent (MDI) quantum key distribution (QKD) network comprising:

a receiver configured to receive optical pulses generated and distributed by a common server;

a modulator configured to modulate the optical pulses for quantum communication;

a transmitter configured to re-transmit the modulated optical pulses to the common server; and

an energy bounding component for limiting Trojan horse attack (THA);

wherein the energy bounding component comprises a power limiter limiting the re-transmitted modulated optical pulses to a maximum intensity during a THA.

10. A method of operating a user system for a measurement-device-independent (MDI) quantum key distribution (QKD) network comprising the steps of:

receiving, at the user system, optical pulses generated and distributed by a common server;

modulating, at the user system, the optical pulses for quantum communication;

re-transmitting, at the user system, the modulated optical pulses to the common server; and

performing energy bounding, at the user system, for limiting Trojan horse attack (THA);

wherein the energy bounding component comprises a power limiter and limiting the THA comprises using the power limiter for limiting the re-transmitted modulated optical pulses to a maximum intensity during a THA.