Title: APPARATUS FOR FREE-SPACE QUANTUM KEY DISTRIBUTION IN DAYLIGHT

Free-space QKD: system overview

Alice

pointing, positionsensitive detector: 15 kHz

timing and control

public channel: wireless ethernet

Bob

timing and control

772 nm

polarized beacon

1550 nm

InGaAs APD: timing

772 nm

635 nm

IR camera: tracking

772 nm

635 nm

pulsed tracking beacon

pointing: position-sensitive detector: 15 kHz

timing pulses/tracking beacon

Fine-pointing mirrors

772 nm

1550 nm

Output light (68, 69) from the lasers that is received by receiving optics (65, 71), where a received timing light pulse (69) is directed to a delay circuit (74) for establishing a timing window for receiving light from the lasers. A computer (65) receives pulses representing the click of the bright timing light pulse (69) and records the start of the time window and the second data bit values in accordance with the first and second polarization states of the output polarized optical data pulses (68), respectively. The receipt of the first and second data bit values is indexed by the bright timing pulse (69).

Abstract: A quantum cryptography apparatus securely generates a key to be used for secure transmission between a sender (61) and a receiver (65) connected by an atmospheric transmission link (66). A laser (69) outputs a timing light pulse; other lasers (68) output polarized data pulses after being enabled by a random bit generator. Output optics (61) transmit light (68, 69) from the lasers that is received by receiving optics (65, 71), where a received timing light pulse (69) is directed to a delay circuit (74) for establishing a timing window for receiving light from the lasers. A computer (65) receives pulses representing the click of the bright timing light pulse (69) and records the start of the time window and the second data bit values in accordance with the first and second polarization states of the output polarized optical data pulses (68), respectively. The receipt of the first and second data bit values is indexed by the bright timing pulse (69).
For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.
**INTERNATIONAL SEARCH REPORT**

**A. CLASSIFICATION OF SUBJECT MATTER**

IPC(7): Ho4L 9/92, 9/94  
US CL: 880/46, 47

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)


Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Advances in Cryptology

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST (USPAT, EPO, JPO, DERWENT), DIALOG, IEEE Xplore

search terms: laser, optical, timing, box car, window, trigger, gate, polarized, pulsed, random, pseudorandom

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Category*</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>US 5,515,438 A (BENNETT et al.) 7 MAY 1996, see column 5, lines 48-50; column 8, lines 24-68; column 9, lines 1-12; and figure 2, items 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, and 21,</td>
<td>1, 3-5</td>
</tr>
<tr>
<td>Y</td>
<td>BENNETT, C.H. et al., &quot;Experimental Quantum Cryptography,&quot; Advances in Cryptology, EuroCrypt '90, 1990, pages 253-265, see page 256.</td>
<td>3, 4</td>
</tr>
<tr>
<td>A</td>
<td></td>
<td>1, 2, 5-14</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C.  
See patent family annex.

- * Special categories of cited documents:  
  - "A" document defining the general state of the art which is not considered to be of particular relevance  
  - "E" earlier document published on or after the international filing date  
  - "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
  - "O" document referring to an oral disclosure, use, exhibition or other means  
  - "P" document published prior to the international filing date but later than the priority date claimed  

- "I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
- "X" document of particular relevance, the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
- "Y" document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
- "M" document member of the same patent family

Date of the actual completion of the international search: 19 OCTOBER 2001

Date of mailing of the international search report: 16 NOV 2001

Name and mailing address of the ISA/US Commissioner of Patents and Trademarks:  
Box PCT  
Washington, D.C. 20231

Facsimile No. (703) 505-5230

Authorized officer:  
JUSTIN T. DARROW

Telephone No. (703) 505-5872

Form PCT/ISA/210 (second sheet) (July 1998)
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>US 5,966,224 A (HUGHES et al.) 12 October 1999, see column 2, lines 35-67 and column 3, lines 1-28.</td>
<td>1-14</td>
</tr>
</tbody>
</table>
B. FIELDS SEARCHED
Minimum documentation searched
Classification System: U.S.

U.S.: 580/56, 57, 46, 47, 54; 706/250, 253, 256

IPC(7): H04L 9/22, 9/24; H04K 1/08; G06F 1/02, 7/58