(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 4 080 352 A8**

(12) **CORRECTED EUROPEAN PATENT APPLICATION**

(15) Correction information:
Corrected version no 1 (W1 A1)
Corrections, see
Bibliography INID code(s) 54

(48) Corrigendum issued on:
30.11.2022 Bulletin 2022/48

(43) Date of publication:
26.10.2022 Bulletin 2022/43

(21) Application number: **22168334.5**

(22) Date of filing: **14.04.2022**

(51) International Patent Classification (IPC):
G06F 7/58 *(2006.01)* ***H04L 9/08*** *(2006.01)*

(52) Cooperative Patent Classification (CPC):
G06F 7/588; H04L 9/0852

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
KH MA MD TN

(30) Priority: **14.04.2021 IT 202100009356**

(71) Applicant: **Fondazione Bruno Kessler**
38122 Trento (IT)

(72) Inventors:
- **MASSARI, Nicola**
  38057 PERGINE VALSUGANA (TN) (IT)
- **PERENZONI, Matteo**
  38068 ROVERETO (TN) (IT)
- **GASPARINI, Leonardo**
  38057 FRAZ. MADRANO, PERGINE VALSUGANA (TN) (IT)
- **TONTINI, Alessandro**
  38052 CALDONAZZO (TN) (IT)
- **ZOU, Yu**
  8050 ZURICH (CH)

(74) Representative: **Marchioro, Paolo**
Studio Bonini S.r.l.
Corso Fogazzaro, 8
36100 Vicenza (IT)

(54) **RANDOM NUMBER GENERATOR, IN PARTICULAR TRULY RANDOM NUMBER GENERATOR OF AN IMPROVED TYPE**

(57) A random number generator (1) comprising, integrated into a single silicon substrate (5), a photon source (2) and a photon detector (3) configured to detect a stream of photons generated by the photon source (2). This random number generator (1) also comprises electronic control means (4) operatively connected to the photon source (2) and to the photon detector (3). The generator provides that the photon source (2) comprises a first SPAD (21), that the photon detector (3) comprises a second SPAD (31) and that the electronic control means (4) are operatively connected to the output of the first SPAD (21) and to the output of the second SPAD (31) so as to receive the output signals (Sout, Sout2) generated by avalanche effects triggered in the first SPAD (21) and in the second SPAD (31) respectively, and are configured to consider as valid for generating a random number only the output signals (Sout2) from the second SPAD (31) generated by avalanche effects triggered in the second SPAD (31) within a correlation time window (T_C), of predetermined duration, starting from the instant in which the electronic control means (4) have detected an avalanche effect in the first SPAD (21).

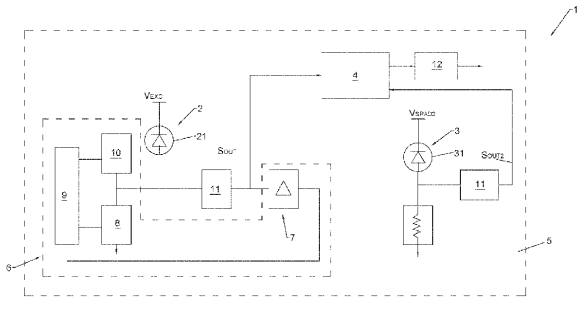

Fig.1

EP 4 080 352 A8