

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la
Propriété Intellectuelle
Bureau international



(10) Numéro de publication internationale
WO 2021/219947 A1

(43) Date de la publication internationale
04 novembre 2021 (04.11.2021)

WIPO | PCT

(51) Classification internationale des brevets :
H04L 9/08 (2006.01)

(72) Inventeur : KAPLAN, Marc ; 13 rue Victor Hugo, 92120
MONTROUGE (FR).

(21) Numéro de la demande internationale :
PCT/FR2021/050662

(74) Mandataire : NOVAGRAAF TECHNOLOGIES ; 2
rue Sarah Bernhardt, CS90017, 92665 ASNIÈRES-SUR-
SEINE CEDEX (FR).

(22) Date de dépôt international :
15 avril 2021 (15.04.2021)

(81) États désignés (sauf indication contraire, pour tout titre de
protection nationale disponible) : AE, AG, AL, AM, AO,
AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA,
CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ,
EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR,
HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP,
KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
FR2004295 30 avril 2020 (30.04.2020) FR

(71) Déposant : VERIQLLOUD [FR/FR] ; 13 rue Victor Hugo,
92120 MONTROUGE (FR).

(54) Title: METHOD FOR SECURELY COMPUTING A LOGICAL AND BETWEEN TWO BITS USING QUANTUM COMMUNICATION

(54) Titre : PROCÉDÉ DE CALCUL D'UN ET LOGIQUE ENTRE DEUX BITS DE MANIÈRE SÉCURISÉE PAR L'UTILISATION DE LA COMMUNICATION QUANTIQUE

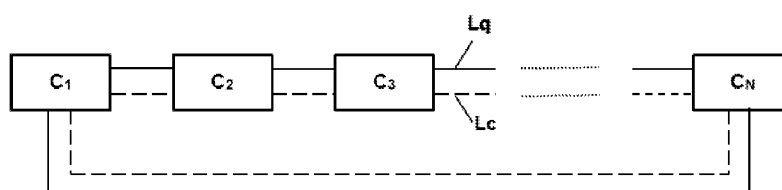


Fig. 1a

(57) Abstract: Method for computing a logical AND between two chosen bits, x_i , x_j , held by first and second participants, including a first phase comprising a step in which said first and second participants determine a first correlation variable and a second correlation variable, each determine a random bit, p and q , and transmit, to said server, a value dependent on said random bit p , q ; a step in which the server prepares a photon in a first state; a step in which said first participant applies a first transformation V_{Up} to said photon; a step in which the second participant applies a second transformation V_{Uq} to said photon; and a step in which the server performs a third transformation $(U^*)_{p+q}$, measures the state of the photon and determines a third correlation variable; and a second phase comprising a step in which said first and second participants exchange a value u_1 , u_2 dependent on the sum of the random bit p , q and the chosen bit x_i , x_j ; and a step in which said first participant computes and delivers a first value $a = + x_i \wedge u_2$, said second participant computes and delivers a second value $b = + x_j \wedge u_1 + u_1 \wedge u_2$ and said server delivers the third correlation value, so that the result of the computation of the logical "and" between said chosen bits may be obtained by summing said first and second values and said third correlation variable.

(57) Abrégé : Procédé pour calculer un ET logique entre deux bits choisis, x_i , x_j détenus par un premier et un second participants, comportant une première phase comprenant une étape dans laquelle lesdits premier et second participants déterminent une première # et seconde # variable de corrélation; déterminent chacun un bit aléatoire, p et q , et transmettent audit serveur, une valeur dépendante dudit bit aléatoire p , q une étape dans laquelle le serveur prépare un photon dans un premier état, une étape dans laquelle ledit premier participant applique une première transformation V_{Up} audit photon, une étape dans laquelle le second participant applique une seconde transformation V_{Uq} audit photon; une étape dans laquelle le serveur effectue une troisième transformation $(U^*)_{p+q}$, mesure l'état du photon et détermine une troisième variable de corrélation #, et, une seconde phase comportant une étape dans laquelle lesdits premier et second participants s'échangent une valeur u_1 , u_2 dépendant de la somme entre le bit aléatoire, p , q , et le bit choisi, x_i , x_j ; une étape dans laquelle ledit premier participant calcule et fournit une première valeur $a = + x_i \wedge u_2$, ledit second participant calcule et

[Suite sur la page suivante]

SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR,
TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

- (84) **États désignés** (*sauf indication contraire, pour tout titre de protection régionale disponible*) : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasién (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée:

— avec rapport de recherche internationale (Art. 21(3))

fournit une seconde valeur $b = \# + x_j \wedge u_1 + u_1 \wedge u_2$ et ledit serveur fournit la troisième variable de corrélation $\#$, de sorte que l'on puisse obtenir le résultat du calcul du « et » logique entre lesdits bits choisi en sommant lesdites première et seconde valeur et ladite troisième variable de corrélation.