PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P1334-1001WO	**FOR FURTHER ACTION**	See Form PCT/IPEA/416
International application No. PCT/GB2019/052268	International filing date *(day/month/year)* 12.08.2019	Priority date *(day/month/year)* 10.08.2018
International Patent Classification (IPC) or national classification and IPC INV. H04L9/08		
Applicant CROALL, Paul Andrew		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 7 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:
   a. ☒ *(sent to the applicant and to the International Bureau)* a total of 8 sheets, as follows:
      ☒ sheets of the description, claims and/or drawings which have been amended and/or sheets containing rectifications authorized by this Authority, unless those sheets were superseded or cancelled, and any accompanying letters (see Rules 46.5, 66.8, 70.16, 91.2, and Section 607 of the Administrative Instructions).
      ☐ sheets containing rectifications, where the decision was made by this Authority not to take them into account because they were not authorized by or notified to this Authority at the time when this Authority began to draw up this report, and any accompanying letters (Rules 66.4bis, 70.2(e), 70.16 and 91.2).
      ☐ superseded sheets and any accompanying letters, where this Authority either considers that the superseding sheets contain an amendment that goes beyond the disclosure in the international application as filed, or the superseding sheets were not accompanied by a letter indicating the basis for the amendments in the application as filed, as indicated in item 4 of Box No. I and the Supplemental Box (see Rule 70.16(b)).
   b. ☐ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing, in the form of an Annex C/ST.25 text file, as indicated in the Supplemental Box Relating to Sequence Listing (see paragraph 3*ter* of Annex C of the Administrative Instructions).

4. This report contains indications relating to the following items:
   - ☒ Box No. I Basis of the report
   - ☐ Box No. II Priority
   - ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - ☐ Box No. IV Lack of unity of invention
   - ☒ Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - ☐ Box No. VI Certain documents cited
   - ☒ Box No. VII Certain defects in the international application
   - ☐ Box No. VIII Certain observations on the international application

Date of submission of the demand	Date of completion of this report
08.06.2020	28.07.2020

Name and mailing address of the international preliminary examining authority:

European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0
Fax: +49 89 2399 - 4465

Authorized officer

Mariggis, Athanasios

Telephone No. +49 89 2399-7118

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/GB2019/052268

Box No. I Basis of the report

1. With regard to the **language**, this report is based on

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of:
   - ☐ international search (under Rules 12.3(a) and 23.1(b))
   - ☐ publication of the international application (under Rule 12.4(a))
   - ☐ international preliminary examination (under Rules 55.2(a) and/or 55.3(a) and (b))

2. With regard to the **elements*** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

Description, Pages

1-23	as originally filed	

Claims, Numbers

1-27	filed with the letter of	09-07-2020

Drawings, Sheets

1/8-8/8	as originally filed	

☐ a sequence listing - see Supplemental Box Relating to Sequence Listing.

3. ☐ The amendments have resulted in the cancellation of:
   - ☐ the description, pages
   - ☐ the claims, Nos.
   - ☐ the drawings, sheets/figs
   - ☐ the sequence listing *(specify)*:

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since either they are considered to go beyond the disclosure as filed, or they were not accompanied by a letter indicating the basis for the amendments in the application as filed, as indicated in the Supplemental Box (Rules 70.2(c) and (c-*bis*)):
   - ☐ the description, pages
   - ☐ the claims, Nos.
   - ☐ the drawings, sheets/figs
   - ☐ the sequence listing *(specify)*:

5. ☐ This report has been established:
   - ☐ taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rules 66.1(d-*bis*) and 70.2(e)).
   - ☐ without taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91(Rules 66.4*bis* and 70.2(e)).

6. ☒ With regard to top-up searches (Rules 66.1*ter* and 70.2(f)):
   - ☒ A top-up search was carried out by this Authority on 10.07.2020 (all discovered documents are listed in the Supplemental Box Relating to Top-up Search).
     - ☐ Additional relevant documents have been discovered during the top-up search.
   - ☐ No top-up search was carried out by this Authority because it would serve no useful purpose.

7. ☐ Supplementary international search report(s) from Authority(ies) has/have been received and taken into account in establishing this report (Rule 45bis.8(b) and (c)).

* *If item 4 applies, some or all of those sheets may be marked "superseded".*

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-27
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-27
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-27
	No:	Claims	

2. Citations and explanations (Rule 70.7):

see separate sheet

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Reference is made to the following documents;the numbering will be adhered to in the rest of the procedure

D1: US 2015/112884 A1 (OSTROVSKY RAFAIL [US] ET AL) 23 April 2015 (2015-04-23)

D2: US 2014/289536 A1 (MACCARTHY JUSTIN [IE] ET AL) 25 September 2014 (2014-09-25)

2 The subject-matter of present independent claims 1, 26 and 27 is new and inventive in the sense of Article 33(2) and (3) PCT.

2.1 Document D1, which is considered to represent the most relevant state of the art, discloses in terms of independent claim 1 (the references in parentheses applying to this document) a computer implemented method of locating one or more members of a familial network (see abstract; paragraphs [0031] to [0036]; figures 1 to 7),

comprising the steps of:

- generating one or more encryption keys derived from a first genomic sequence (see paragraphs [0032] and [0111] to [0115]; figures 1 to 7);

- encrypting a message using the or each encryption key to form an encrypted message (see paragraphs [0032] and [0111] to [0115]; figures 1 to 7);

- sending the encrypted message to one or more remote devices wherein decrypting the encrypted message at the one or more remote devices uses one or more encryption keys derived from a second genomic sequence (see paragraphs [0032] and [0111] to [0115]; figures 1 to 7); and

- receiving a confirmation regarding whether the decryption of the encrypted message was successful by any of the one or more remote devices (see paragraphs [0032] and [0111] to [0115]; figures 1 to 7).

2.2 Document D1, however, does not disclose nor suggest the following **underlined and highlighted** features of claim 1:

-- **wherein, sending the encrypted message comprises generating a *genetic* address from the first genomic sequence**.

2.3 In the light of the above, the problem to be solved can thus be defined, as how to provide a secure, fast and more efficient mechanism for facilitating search and detection of "users" wishing contacts within a "particular biological range" (i.e. to find biologically close relatives).

2.4 This problem is solved by the non-obvious combination of the features as defined in present claim 1.

More particularly, the essential idea of the present invention is based on the fact that, If two individuals share more than a predetermined proportion of their **genomic sequences**, it is likely to be indicative of the **biological closeness** between those two individuals. Thus, it may be advantageous to contact only such relatives, otherwise a large number of spurious messages will be sent and the accuracy of finding one's relatives reduced.

Therefore, the claimed arrangement, also referred to as the **chromosomal identification** arrangement, provides the ability to communicate with potentially lost family members, using the DNA of a sender (or "user") without making any DNA public. The sender may comprise a person who is entering its DNA into the chromosomal identification arrangement in order to make use of the arrangement provided herein. For example, a lost family member may be identified and reconnected with. As genomic data may be considered private, it is important to attempt to very carefully limit who can access the data. **To this end, a sequenced genome comprising or derived from the DNA of the user may be used to create a *genetic* address**.

Based on the above, the **chromosomal identification** arrangement enables a distributed database of messages to be held across a distributed network of nodes, **including DNA addresses**. A DNA address is the sender's address, but also sender and receiver either share a fragment of their respective DNA addresses, or a respective portion of their DNA addresses comprise one or more numbers which are of a **predetermined closeness** to each other. Each

node sends each message it receives classically to one or more other nodes. The node sends the message to the nodes that, according to the data known, have messages coming from or going to those address fragments.

This distributed processing technique leads to close relatives' messages meeting each other, converging and hence reaching the same nodes.

Furthermore, generating the index sorted by genetic DNA addresses and accepting the closest available, thereby using one or more distributed processing achievements, can significantly reduce the time taken to find a "relative", when compared with conventional methods of searching. Nearest "relatives" using the chromosomal identification arrangement can, therefore, be connected. "Non-users" (i.e. not interested "users") will not be connected, and so can remain hidden from their "relatives" using the present claimed arrangement.

By contrast, documents D1 and D2 are totally silent regarding the aforementioned distinguishing features as well as regarding their technical effects.

2.5 Consequently, since none of the cited documents (D1 and D2) discloses nor suggests the combination of features as claimed in present claim 1, the subject-matter of present claim 1 is considered to be novel and inventive (Article 33(2) and (3) PCT).

2.6 The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent apparatus claims 26 and 27, which therefore are also considered as novel and inventive (Article 33(2) and (3) PCT).

3 The dependent claims derive their patentability from the independent claims to which they refer back.

Re Item VII

Certain defects in the international application (form or content)

4 In addition, the following formal requirements should be attended to in the amended application to be filed:

4.1 All claims should include reference signs relating to the technical features referred to therein (Rule 6.2(b) PCT).

4.2 The opening part of the description should be modified to bring it into agreement with any amended independent claim (Rule 5.1(a)(iii) PCT).

4.3 In order to meet more fully the requirements of Rule 5.1(a)(ii) PCT, the cited documents D1 and D2 should be acknowledged and briefly discussed in the opening part of the description.

Barnes IP Limited
Castle Hill House, 12 Castle Hill,
Windsor, Berkshire SL4 1PD,
United Kingdom
T: 0203 858 0810 F: 01753 260 150
E: contactus@barnesip.co.uk

International Preliminary Examination Authority
European Patent Office
Postbus 5818
2280 HV Rijswijk
The Netherlands

Our Ref: **P1334-1001WO**
Your Ref: **PCT/GB2019/052268**
Date: **09 July 2020**

Via: **EPO ONLINE FILING ONLY**

Dear Sirs,

PCT App. No.: **PCT/GB2019/052268**
Applicant: **CROALL, Paul Andrew**
Title: **Chromosomal Identification**

Following the demand for International Preliminary Examination under PCT Article 31 filed for the above-referenced application on 08 June 2020, and the invitation to submit amendments of 16 June 2020, we hereby submit observations and amendments to address the objections raised in the Written Opinion and request that the Examiner reconsiders the merits of the present application.

Amendments

In accordance with PCT Rule 66.8(c), the enclosed amended set of claims is intended to replace the claims as originally filed. A marked-up version of the amended claims clearly showing the amendments made to the originally filed claims is also attached for the Examiner's convenience.

➔ Please exchange the clean copy of the amended claims submitted with this letter with those claims presently on file.

Basis for Amendments

Claim 1 has been amended to recite:

> 1. A computer implemented method of locating one or more members of a familial network, comprising the steps of:
>
> generating one or more encryption keys derived from a first genomic sequence;
>
> encrypting a message using the or each encryption key to form an encrypted message;
>
> sending the encrypted message to one or more remote devices wherein decrypting the encrypted message at the one or more remote devices uses one or more encryption keys derived from a second genomic sequence; and

receiving a confirmation regarding whether the decryption of the encrypted message was successful by any of the one or more remote devices

wherein, sending the encrypted message comprises generating a genetic address from the first genomic sequence.

Basis for this amendment can be found on, page 2, lines 17 – 18, page 7, lines 21 – 26, and page 8, lines 31 – 32 of the description as originally filed.

Corresponding amendments have also been made to independent clams 26 and 27.

Novelty and Inventive Step

In response to the novelty and inventive step objections raised in the Written Opinion in Item V, the applicant respectfully submits that the features recited by the amended claims are not all disclosed or hinted at by the cited prior art documents, either alone or in combination

In the Written Opinion, the Examiner refers to two prior art documents. For the Examiner's ease, the documents are referred to below using the same references already allocated by the Examiner in the Written Opinion, repeated here for ease of reference as follows:

D1: US 2015/112884 A1
D2: US 2014/289536 A1

Use of Genetic Address & Confirmatory Step Not Disclosed in Prior Art Documents

Amended claim 1 now recites "wherein, sending the encrypted message comprises generating a genetic address from the first genomic sequence".

As one would expect, to route a message requires a destination address, or at the very least a direction in which to pass the message. In some instances, this may include or facilitate moving a message closer and closer, step by step, to the intended recipient. In the claimed invention, this type of routing is achieved using a genetic address, or a "DNA Address". The applicant respectfully submits that none of the cited prior art documents teach or mention any such concept. Neither of documents D1 or D2 disclose a routing mechanism using a genetic address derived from a genomic sequence.

Additionally, and with reference to the definition of the terminology clarified herein, amended claim 1 recites "receiving a confirmation regarding whether the decryption of the encrypted message was successful by any of the one or more remote devices". Although the Examiner alleges this feature is disclosed in paragraphs [0032] and [0111 – 0115], and in Figures 1 – 7, of document D1, and disclosed in Figure 3 of document D2, the applicant respectfully disagrees. Neither prior document mentions transmitting data regarding successful decryption. The Examiner's focus on document D1 appears to revolve around the use of the term 'fuzzy encryption', which will be discussed in more detail below. In any case, the applicant respectfully submits that there is no mention of a confirmatory step where successful or unsuccessful decryption is relayed back to a remote device. In document D2, although there is a disclosure of "transmitting, from the processor, the match data" [0090], this does not transmit data regarding successful decryption.

Given the use of routing messages using a genetic address in the invention defined by the amended claims, a robust confirmation mechanism is necessary for secure routing of messages. This is not a feature taught or mentioned in the cited prior art documents as the methods of the prior art rely on leaking a confidential data along the route it tries. This could enable a bad actor to send a forged reply back from where a message came, claiming a family relationship which is not true, but would be verified by a fuzzy match in document D1 or a matching base pair in document D2. In contrast, the claimed invention's lack of such leakage prevents that possibility and in addition the confirmation does not merely indicate that a message could not be sent, but rather that it would be detected as unencryptable and therefore unrelated.

Use of Encryption vs Scrambling

Additionally, the cited prior art documents appear to teach methods of using public keys and/or private keys. The applicant submits that this is not the same as the "encryption keys" as described in the claimed invention, but instead what is disclosed in the prior art documents is a scrambled partial DNA sequence which can leak confidential DNA data. Since the methods of the cited prior art rely on matching using the leaked data, these methods in fact make confidential information public because the method disclosed do not actually encrypt the payload – the DNA data.

A skilled person would appreciate the distinction between actual encryption of a message and merely scrambling a message. For example, scrambling a message typically uses a mathematical convolution operation to disguise the message which does not require an encryption key nor can the scrambled message be considered to be the encryption key, particularly in light of the methods described in each prior art document – which as mentioned above both relate to matching. In particular, rather than decryption, document D2 [0090] only describes a comparison of base-pair matching.

In document D1, the term 'fuzzy encryption' is used as description of the disclosed way of scrambling sequenced DNA and revealing or leaking fragments of the sequence for comparison. The applicant respectfully submits that the method disclosed in document D1 is therefore entirely different since it conflates the encryption key, the message, and the sequence – they are all considered to be the same in D1.

Thus, the methods disclosed in documents D1 and D2 scramble the message, where the messages are rearranged in a reversable form (for example to those who know the algorithm), and partially disclose the data by leaking a part of the data to assist matching. These steps are incorrectly referred to as encryption, rather than more correctly as creating a scrambled payload. It is submitted that the use of the term "encryption" in documents D1 and D2 is therefore a misnomer, as what would be considered encryption by a skilled person does not appear to be taking place in the methods disclosed.

In contrast, the invention as defined in the amended claims generates one or more encryption keys derived from a first genomic sequences (for later decryption and independently of the message to be encrypted) and encrypts the message using the one or more encryption keys. In this way, the claimed invention has a clear distinction between the encryption key, the message, sequenced DNA and the genetic address. In the invention defined by the amended claims, this ensures knowing or having a

message of the claimed invention does not reveal or leak any base pairs or any parts of the sequenced DNA data.

Conclusion

Therefore, the methods disclosed in the prior art documents do not anticipate the invention defined by the amended claims, nor hint at the combination of the method steps recited in the amended claims.

Thus, it is submitted that the present invention as defined by the amended claims is both novel and inventive over the cited prior art documents, alone or in combination.

Next Steps

It is respectfully requested that, on the basis of the above submissions, the application is reconsidered and a positive IPER for the application is requested.

However, should the Examiner disagree with or have any queries in relation to any of the above submissions, we kindly request the opportunity for either a telephone consultation with the Examiner or a further written communication, in line with PCT Rules 66.6 and 66.4 respectively, before issuing a negative IPER.

Yours faithfully,

Suchit Amin
For and on behalf of
Barnes IP Limited
Association No 982

Enclosures: Amended Claims (clean & tracked)

CLAIMS:

1. A computer implemented method of locating one or more members of a familial network, comprising the steps of:

generating one or more encryption keys derived from a first genomic sequence;

encrypting a message using the or each encryption key to form an encrypted message;

sending the encrypted message to one or more remote devices wherein decrypting the encrypted message at the one or more remote devices uses one or more encryption keys derived from a second genomic sequence; and

receiving a confirmation regarding whether the decryption of the encrypted message was successful by any of the one or more remote devices

wherein, sending the encrypted message comprises generating a genetic address from the first genomic sequence.

2. The method of claim 1, further comprising the steps of:

receiving an input comprising a first genomic sequence; and

generating one or more encryption keys based on the input.

3. The method of any preceding claim, wherein the step of decrypting the encrypted message at the one or more remote devices uses one or more encryption keys derived from one or more further genomic sequences.

4. The method of any preceding claim, wherein one or more of the encryption keys comprises:

a first encryption key for a verbatim encryption algorithm, and

a second encryption key for a unique encryption algorithm.

5. The method of claim 4, wherein the first encryption key is used in relation to:

one or more mitochondria;

a first X chromosome; and

a second X chromosome or a Y chromosome,

to form three verbatim algorithmically generated ciphers in relation to the first genomic sequence.

6. The method of claim 4, wherein the second encryption key is used to encrypt the message using a combination of chromosomes 1 through 22 comprised in the first genomic sequence.

7. The method of any preceding claim, wherein the step of sending the encrypted message is performed using one or more outputs derived from the first genomic sequence.

8. The method of any preceding claim, wherein the successful decryption of the encrypted message is indicative of a predetermined level of familial closeness.

9. The method of any preceding claim, wherein the first and/or second genomic sequence comprises at least a portion of a genome sequence.

10. The method of any preceding claim, wherein a genomic sequence comprises four bases comprising one or more of: guanine (G), cytosine (C), adenine (A), thymine (T), and/or uracil (U).

11. The method of claim 10, wherein the four bases are mapped to a binary sequence.

12. The method of claim 11, wherein the binary sequence comprises two forms: pressed and/or unpressed.

13. The method of any preceding claim, wherein the input comprises the number of one or more of the four bases.

14. The method of any preceding claim, wherein the decryption of the encrypted message is successful only if a predetermined proportion of the first genomic sequence corresponds to the second genomic sequence.

15. The method of claim 14, wherein the predetermined proportion reflects the level of familial relationship between an owner of the first genomic sequence and an owner of the second genomic sequence.

16. The method of any preceding claim, wherein the step of sending the encrypted message comprises forming an array of three by four integers and a unique individual hashed integer identifier.

17. The method of claim 16, wherein the unique individual hashed integer is a hash of an entire genome sequence.

18. The method of claim 17, further comprising a superimposition of a timestamp of the sequencing date.

19. The method of any preceding claim, wherein the step of encrypting the message comprises the use of a binary large object of prime sized words (BoPSW).

20. The method of any preceding claim, wherein the or each of the one or more nodes of the distributed network of nodes is only operable to send the encrypted message only the first time that the encrypted message is received by the or each node.

21. The method of any preceding claim, wherein the or each node of the distributed network has an associated user.

22. The method of any preceding claim, further comprising the step of:

outputting a measure of genetic distance between the first genomic sequence and the second genomic sequence.

23. The method of claim 22, wherein the measure of genetic distance is determined using a DNA address.

24. The method of any preceding claim, wherein the encrypted message is stored for a portion of time on a remote server.

25. The method of claim 24, wherein the decryption of the encrypted message following the step of sending the encrypted message takes place after a time delay.

26. A familial network location apparatus, comprising:

a processor operable to:

generate one or more encryption keys derived from a first genomic sequence;

encrypt a message using the or each encryption key to form an encrypted message;

send the encrypted message to one or more devices wherein decrypting the encrypted message at the one or more devices uses one or more encryption keys derived from a second genomic sequence; and

receive a confirmation regarding whether the decryption of the encrypted message was successful by any of the one or more remote devices

wherein, sending the encrypted message comprises generating a genetic address from the first genomic sequence.

27. A system to locate one or more members of a familial network, comprising:

a processor operable to:

generate one or more encryption keys derived from a first genomic sequence;

encrypt a message using the or each encryption key to form an encrypted message;

send the encrypted message to one or more devices wherein decrypting the encrypted message at the one or more devices uses one or more encryption keys derived from a second genomic sequence; and

receive a confirmation regarding whether the decryption of the encrypted message was successful by any of the one or more remote devices

wherein, sending the encrypted message comprises generating a genetic address from the first genomic sequence.