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

(11) **EP 4 283 922 A3**

(12) **EUROPEAN PATENT APPLICATION**

(88) Date of publication A3:
28.02.2024 Bulletin 2024/09

(43) Date of publication A2:
29.11.2023 Bulletin 2023/48

(21) Application number: **23193892.9**

(22) Date of filing: **15.08.2018**

(51) International Patent Classification (IPC):
H04L 9/00 *(2022.01)* ***H04L 9/06*** *(2006.01)*
H04L 9/08 *(2006.01)* ***H04L 9/30*** *(2006.01)*
H04L 9/32 *(2006.01)*

(52) Cooperative Patent Classification (CPC):
H04L 9/0656; H04L 9/0816; H04L 9/0872; H04L 9/3066; H04L 9/3239; H04L 9/3252; H04L 9/50

(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

(30) Priority: **23.08.2017 GB 201713499**
23.08.2017 PCT/IB2017/055073

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
18765196.3 / 3 673 610

(71) Applicant: **nChain Licensing AG**
6300 Zug (CH)

(72) Inventor: **WRIGHT, Craig Steven**
Cardiff, CF10 2HH (GB)

(74) Representative: **Murgitroyd & Company**
Murgitroyd House
165-169 Scotland Street
Glasgow G5 8PL (GB)

(54) COMPUTER-IMPLEMENTED SYSTEM AND METHOD FOR HIGHLY SECURE, HIGH SPEED ENCRYPTION AND TRANSMISSION OF DATA

(57) The present disclosure relates to highly secure, high speed encryption methodologies suitable for applications such as media streaming, streamed virtual private network (VPN) services, large file transfers and the like. For example, encryption methodologies as described herein can provide stream ciphers for streaming data from, for example, a media service provider to a plurality of users. Certain configurations provide wire speed single use encryption. The methodologies as described herein are suited for use with blockchain (e.g. Bitcoin) technologies.

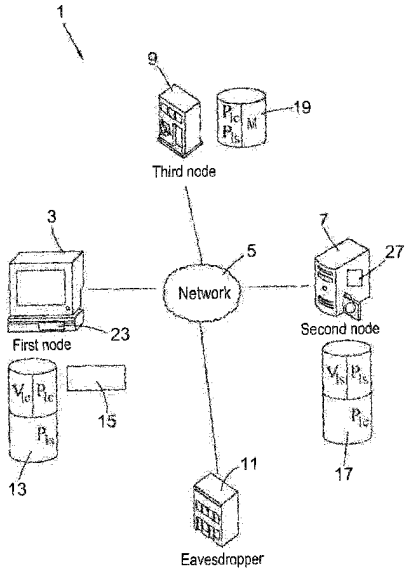

Fig. 1

EP 4 283 922 A3

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 23 19 3892

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
Y	"Chapter 12: Key Establishment Protocols ED - Menezes A J; Van Oorschot P C; Vanstone S A", HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, PAGE(S) 489 - 541 , 1 October 1996 (1996-10-01), XP001525012, ISBN: 978-0-8493-8523-0 Retrieved from the Internet: URL:http://www.cacr.math.uwaterloo.ca/hac/ * Section 12.6.1, (i) and (iii) * -----	1-15	INV. H04L9/00 H04L9/06 H04L9/08 H04L9/30 H04L9/32
Y	EP 1 063 811 A1 (HITACHI EUROP LTD [GB]) 27 December 2000 (2000-12-27) * abstract; figures 1-6 * * paragraphs [0026] - [0037] * -----	1-15	
A	US 8 165 303 B1 (STEELE JOSEPH D [US] ET AL) 24 April 2012 (2012-04-24) * abstract; figures 1-3 * * column 2, line 55 - column 4, line 48 * -----	1-15	TECHNICAL FIELDS SEARCHED (IPC) H04L
A	FLEISCHHACKER NILS ET AL: "Efficient Unlinkable Sanitizable Signatures from Signatures with Re-randomizable Keys", 18 February 2016 (2016-02-18), ECCV 2016 CONFERENCE; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER INTERNATIONAL PUBLISHING, CHAM, PAGE(S) 301 - 330, XP047335884, ISSN: 0302-9743 ISBN: 978-3-319-69952-3 [retrieved on 2016-02-18] * Section 3. * ----- -/--	1-15	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	16 January 2024	Wolters, Robert

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons
& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 23 19 3892

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	GUY ZYSKIND ET AL: "Decentralizing Privacy: Using Blockchain to Protect Personal Data", THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC. (IEEE) CONFERENCE PROCEEDINGS, 1 May 2015 (2015-05-01), page 180, XP055360065, Piscataway * the whole document *	1-15	

TECHNICAL FIELDS SEARCHED (IPC)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	16 January 2024	Wolters, Robert

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 23 19 3892

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

16-01-2024

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1063811 A1	27-12-2000	AT E403992 T1	15-08-2008
		EP 1063811 A1	27-12-2000
		JP 3901909 B2	04-04-2007
		JP 2001007800 A	12-01-2001
		US 7177424 B1	13-02-2007
US 8165303 B1	24-04-2012	US 8165303 B1	24-04-2012
		US 2014032909 A1	30-01-2014

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82