(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2012 年 9 月 27 日 (27.09.2012)

WIPO | PCT

(10) 国际公布号
WO 2012/126432 A3

(51) 国际专利分类号:
H04L 9/08 (2006.01)

(21) 国际申请号: PCT/CN2012/076069

(22) 国际申请日: 2012 年 5 月 29 日 (29.05.2012)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人 (对除美国外的所有指定国): **华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **卢胜文 (LU, Shengwen)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: **北京龙双利达知识产权代理有限公司 (LONGSUN LEAD IP LTD.)**; 中国北京市海淀区丹棱街 16 号海兴大厦 C 座 1108, Beijing 100080 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (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, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

[见续页]

(54) **Title**: METHOD, DEVICE AND SYSTEM FOR DATA TRANSMISSION

(54) **发明名称** : 数据传输的方法、设备和系统

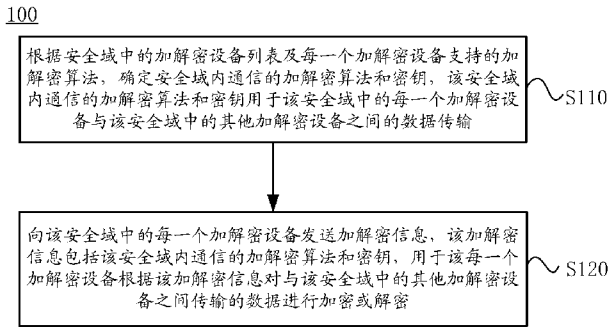

图 1 / Fig.1

S110 DETERMINING THE COMMUNICATIONS ENCRYPTION/DECRYPTION ALGORITHM AND KEY WITHIN THE SECURITY DOMAIN AND AN ENCRYPTION/DECRYPTION ALGORITHM SUPPORTED BY EVERY ENCRYPTION/DECRYPTION DEVICE ACCORDING TO AN ENCRYPTION/DECRYPTION DEVICE LIST WITHIN THE SECURITY DOMAIN, WHERE THE COMMUNICATIONS ENCRYPTION/DECRYPTION ALGORITHM AND WITHIN THE SECURITY DOMAIN ARE USED TO TRANSMIT DATA WITHIN THE SECURITY DOMAIN BETWEEN ENCRYPTION/DECRYPTION DEVICES

S120 SENDING TO EACH ENCRYPTION/DECRYPTION DEVICE WITHIN THE SECURITY DOMAIN ENCRYPTION/DECRYPTION INFORMATION CONTAINING THE COMMUNICATIONS ENCRYPTION/DECRYPTION ALGORITHM AND KEY WITHIN THE SECURITY DOMAIN USED BY EVERY ENCRYPTION/DECRYPTION DEVICE ACCORDING TO THE ENCRYPTION/DECRYPTION INFORMATION TO ENCRYPT OR DECRYPT DATA TRANSMITTED BETWEEN OTHER ENCRYPTION/DECRYPTION DEVICES IN THE SECURITY DOMAIN

(57) Abstract: The embodiment of the present invention discloses a method, a device and a system for data transmission, wherein the method determines the communications encryption/decryption algorithm and key within the security domain and an encryption/decryption algorithm supported by every encryption/decryption device according to an encryption/decryption device list within the security domain, wherein the communications encryption/decryption algorithm within the security domain is used to transmit data within the security domain between encryption/decryption devices; sends to each encryption/decryption device within the security domain encryption/decryption information containing the communications encryption/decryption algorithm and key within the security domain used by every encryption/decryption device according to the encryption/decryption information to encrypt or decrypt data transmitted between other encryption/decryption devices in the security domain. The embodiment of the present invention, being a data transmission method, a device and a system for determining via a security management device the encryption/decryption algorithm and key for data transmission within the security domain, can guarantee secure data transmission in the security domain while consolidating, coordinating, and managing algorithms and keys for data transmission within the security domain, thereby alleviating key coordination problems.

(57) 摘要:

[见续页]

WO 2012/126432 A3

(88) 国际检索报告公布日期: 2013 年 5 月 2 日

— 在修改权利要求的期限届满之前进行，在收到该修改后将重新公布(细则 48.2(h))。

— 根据申请人的请求，在条约第 21 条(2)(a)所规定的期限届满之前进行。

本发明实施例提供了一种数据传输的方法、设备和系统。该方法包括：根据安全域中的加解密设备列表及每一个加解密设备支持的加解密算法，确定安全域内通信的加解密算法和密钥，该安全域内通信的加解密算法和密钥用于该安全域中的加解密设备之间的数据传输；向该安全域中的每一个加解密设备发送加解密信息，该加解密信息包括该安全域内通信的加解密算法和密钥，用于该每一个加解密设备根据该加解密信息对与该安全域中的其他加解密设备之间传输的数据进行加密或解密。本发明实施例的数据传输的方法、设备和系统，通过安全管理设备确定用于安全域内数据传输的加解密算法和密钥，能够在保证安全域内数据传输安全的同时，集中协商和管理安全域内数据传输的算法和密钥，减少密钥协商的压力。

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2012/076069

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08 (2006.01) i

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)

IPC: H04L

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

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

CNABS, CNTXT, CNKI, VEN, USTXT: safety, secur+, domain, group, encrypt+, decrypt+, centr+, algorithm, key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7594262 B2 (SECURE COMPUTING CORP.) 22 September 2009 (22.09.2009) see description, column 5, line 1 to line 42, column 6, line 3 to column 10, line 39 and figures 1B, 2-6	1-32
X	CN 1731720 A (BEIJING ELECTRONIC SCI & TECHNOLOGY INST et al.) 08 February 2006 (08.02.2006) see description, page 3, line 7 to page 6, line 3 and figures1-5	1-32
A	CN 101374153 A (CHINA MOBILE COMMUNICATION CORP et al.) 25 February 2009 (25.02.2009) the whole document	1-32
A	CN 101764742 A (FUJIAN XINGWANG RUIJIE NETWORK CO LTD) 30 June 2010 (30.06.2010) the whole document	1-32
A	WO 2010033353 A2 (MOTOROLA INC et al.) 25 March 2010 (25.03.2010) the whole document	1-32

☐ 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 application or patent but 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

"T" 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

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 February 2013 (21.02.2013)	07 March 2013 (07.03.2013)
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10)62019451	Authorized officer ZOU, Feifei Telephone No. (86-10)62411263

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2012/076069

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US 7594262 B2	22.09.2009	US 2004044891 A1	04.03.2004
CN 1731720 A	08.02.2006	None	
CN 101374153 A	25.02.2009	CN 101374153 B	29.02.2012
CN 101764742 A	30.06.2010	None	
WO 2010033353 A2	25.03.2010	EP 2329663 A2	08.06.2011
		WO 2010033353 A3	20.05.2010
		US 2010074446 A1	25.03.2010
		AU 2009293583 A1	25.03.2010
		CA 2729046 A1	25.03.2010

国际检索报告

国际申请号
PCT/CN2012/076069

A. 主题的分类

H04L9/08（2006.01）i

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC：H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNABS，CNTXT，CNKI，VEN，USTXT：安全域，加密，解密，加解密，集中，统一，算法，密钥，safety，secur+，domain，group，encrypt+，decrypt+，centr+，algorithm，key

C. 相关文件

类　型*	引用文件，必要时，指明相关段落	相关的权利要求
X	US7594262B2（SECURE COMPUTING CORP）22.9 月 2009（22.09.2009）参见说明书第 5 栏第 1 行至第 42 行，第 6 栏第 3 行至第 10 栏第 39 行及附图 1B，2-6	1-32
X	CN1731720A（北京电子科技学院等）08.2 月 2006（08.02.2006）参见说明书第 3 页第 7 行至第 6 页第 3 行及附图 1-5	1-32
A	CN101374153A（中国移动通信集团公司等）25.2 月 2009（25.02.2009）参见全文	1-32
A	CN101764742A（福建星网锐捷网络有限公司）30.6 月 2010（30.06.2010）参见全文	1-32
A	WO2010033353A2（MOTOROLA INC et al.）25.3 月 2010（25.03.2010）参见全文	1-32

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
21.2 月 2013（21.02.2013）	**07.3 月 2013 (07.03.2013)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号：　(86-10)62019451	受权官员 邹菲菲 电话号码：(86-10) **010-62411263**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2012/076069

检索报告中引用的专利文件	公布日期	同族专利	公布日期
US7594262B2	22.09.2009	US2004044891A1	04.03.2004
CN1731720A	08.02.2006	无	
CN101374153A	25.02.2009	CN101374153B	29.02.2012
CN101764742A	30.06.2010	无	
WO2010033353A2	25.03.2010	EP2329663A2	08.06.2011
		WO2010033353A3	20.05.2010
		US2010074446A1	25.03.2010
		AU2009293583A1	25.03.2010
		CA2729046A1	25.03.2010