(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
2013 年 4 月 18 日 (18.04.2013)

WIPO | PCT

(10) 国际公布号
WO 2013/053078 A1

(51) 国际专利分类号:
H04L 9/06 (2006.01)

(21) 国际申请号: PCT/CN2011/001694

(22) 国际申请日: 2011 年 10 月 10 日 (10.10.2011)

(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): **厦门简帛信息科技有限公司 (XIAMEN GEEBOO INFORMATION TECHNOLOGY CO., LTD)** [CN/CN]; 中国福建省厦门市软件园二期望海路 63 号 802B 单元, Fujian 361000 (CN)。

(72) 发明人; 及
(71) 申请人 : **黄金旭 (HUANG, Jinxu)** [CN/CN]; 中国北京海淀区泉宗路 10 号 C-1-1503, Beijing 100098 (CN)。

(74) 代理人: **北京国帆知识产权代理事务所（普通合伙） (BEIJING GUOFAN I. P. AGENCY)**; 中国北京市石景山区八大处高科技园区西井路 3 号三号楼 576 房间, Beijing 100043 (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, MD, 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))。

(54) **Title**: ENCRYPTION METHOD

(54) **发明名称** : 一种加密方法

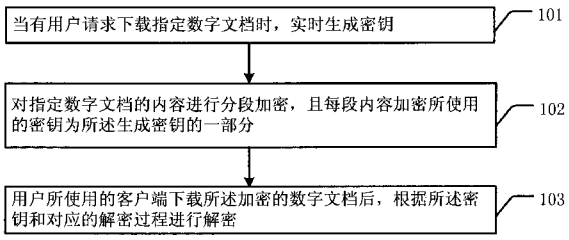

图 1 / **Fig.1**

101 WHEN THE USER REQUESTS TO DOWNLOAD THE DESIGNATED DIGITAL FILE, GENERATION IN REAL TIME OF THE ENCRYPTION KEY
102 ENCRYPTION OF THE SEGMENTS OF THE CONTENT OF THE DESIGNATED DIGITAL FILE, WHERE THE ENCRYPTION KEY USED FOR THE ENCRYPTION OF EACH SEGMENT IS A PART OF THE ENCRYPTION KEY GENERATED
103 WHEN THE ENCRYPTED DIGITAL FILE IS DOWNLOADED BY THE CLIENT TERMINAL THAT IS USED BY THE USER, DECRYPTION ON THE BASIS OF THE ENCRYPTION KEY AND OF THE CORRESPONDING DECRYPTION PROCESS

(57) **Abstract**: Disclosed is an encryption method. The method comprises: when a user requests to download a designated digital file, generating in real time an encryption key; encrypting segments of the content of the designated digital file, where the encryption key used for the encryption of each segment of the content is a part of the encryption key generated, and, when the encrypted electronic file is downloaded by a client terminal that is used by the user, decrypting on the basis of the encryption key and of a corresponding decryption process. The encryption method of the present invention cannot be cracked easily, thus improving the security of the digital file.

(57) **摘要**: 本发明公开了一种加密方法。该方法包括：当有用户请求下载指定数字文档时，实时生成密钥；对指定数字文档的内容进行分段加密，且每段内容加密所使用的密钥为所述生成密钥的一部分；用户所使用的客户端下载已加密的电子文档后，根据所述密钥和对应的解密过程进行解密。本发明的这种加密方法不易被破解，增加了数字文档的安全性。

WO 2013/053078 A1

说 明 书

一种加密方法

技术领域

本发明涉及网络信息安全技术领域，特别是涉及一种加密方法。

背景技术

在当前的互联网信息时代，人们对信息的需求越来越大。而数字文档作为一种数字信息的载体，也成为了现代人们阅读习惯中不可或缺的一份。

而现有的数字文档加密方法总是存在很多不足，容易被破解，使得数字文档的提供商和版权所有者的利益受到损害。因此需要提供一种更安全的加密方法。

发明内容

本发明提供了一种加密方法，该加密方法不易被破解，增加了数字文档的安全性。

为达到上述目的，本发明的技术方案是这样实现的：

本发明公开了一种加密方法，该方法包括：

当有用户请求下载指定数字文档时，生成密钥；

对指定数字文档的内容进行分段加密，且每段内容加密所使用的密钥为所述生成密钥的一部分；

用户所使用的客户端下载所述加密的数字文档后，根据所述密钥和对应的解密过程进行解密。

在上述方法中，所述对指定数字文档的内容进行分段加密，且每段内容加密所使用的密钥为所述生成密钥的一部分包括以下步骤：

A、跳过数字文档内容的文件头部分；令i＝1；

B、从所跳过的内容之后按顺序读取N_i字节的二进制内容，从所述生成密钥获取一定位数的内容作为本次密钥，用本次密钥对读

取的二进制内容进行加密；

C、跳过M_i位的二进制内容；

D、判断对数字文档内容的加密是否完成，是则结束流程，否则令i＝i＋1，返回步骤B。

在上述方法中，N_i由与所述指定数字文档相关的信息确定。

在上述方法中，M_i等于所述指定数字文档的标识的位数。

在上述方法中，所述步骤B中的从所述生成密钥获取一定位数的内容作为本次密钥包括：

如果从所述生成密钥获取到零位的内容，则不对本次所读取的二进制内容进行加密。

在上述方法中，所述与指定数字文档相关的信息包括：所述指定数字文档的固有信息的一种或多种。

由上述可见，本发明这种当有用户请求下载指定数字文档时，生成密钥；对指定数字文档的内容进行分段加密，且每段内容加密所使用的密钥为所述生成密钥的一部分；用户在客户端下载所述加密的数字文档后，根据所述密钥和对应的解密过程进行解密的技术方案，使得该加密方法不易被破解，增加了数字文档的安全性。

附图说明

图1是本发明实施例中的一种加密方法的流程图。

图2是本发明实施例中的对数字文档内容进行加密的示意图。

具体实施方式

为了使本发明的目的、技术方案和优点更加清楚，下面结合附图和具体实施例对本发明进行详细描述。

图1是本发明实施例中的一种加密方法的流程图。如图1所示，该方法包括以下步骤：

步骤101，当有用户请求下载指定数字文档时，实时生成密钥。

本步骤当中，具体可以根据现有的密钥生成方式实时生成密钥，具体的密钥生成方法本发明中不予限定。这里实时是指在有用户请求的当时生成密钥，而不是事前生成好的。

步骤102，对指定数字文档的内容进行分段加密，且每段内容加密所使用的密钥为所述生成密钥的一部分。

步骤103，用户所使用的客户端下载所述加密的数字文档后，根据所述密钥和对应的解密过程进行解密。

图1所述的加密方法不易被破解，增加了数字文档的安全性。

图1所示方法中的步骤102所述的对数字文档内容进行分段加密，且每段内容加密所使用的密钥为所述生成密钥的一部分具体可以包括以下步骤：

A、跳过数字文档内容的文件头部分；令i＝1；

B、从所跳过的内容之后按顺序读取N_i字节的二进制内容，从所述生成密钥获取一定位数的内容作为本次密钥，用本次密钥对读取的二进制内容进行加密；

C、跳过M_i位的二进制内容；

D、判断对数字文档内容的加密是否完成，是则结束流程，否则令i＝i＋1，返回步骤B。

其中，N_i由与所述指定数字文档相关的信息确定，其中所述与指定数字文档相关的信息包括：所述指定数字文档的固有信息的一种或多种；M_i等于根据所述指定数字文档的固有信息动态生成的固定位数，；所述步骤B中如果从所述生成密钥获取到零位的内容，则不对本次所读取的二进制内容进行加密。

图2是本发明实施例中的对数字文档内容进行加密的示意图。如图2所示，用一定长度的线段表示数字文档的内容，标示在线段下面的是跳过的内容，标示在线段上面的是进行加密的内容。这里以生成的密钥为128位为例进行说明。

在图2所示的实施例中：首先跳过文件头部分，读取N_1字节的内容，从所生成的128位的密钥中获取一部分，如32位的内容作为密钥对N_1字节的内容进行加密；跳过M_1位的内容，读取N_2字节的内容，从所生成的128位的密钥中获取一部分，如64位的内容作为密钥对N_2字节的内容进行加密；跳过M_2位的内容，读取N_3字节的内容，从所生成的128位的密钥中获取一部分（可以是全部），如128

位的内容作为密钥对N_3字节的内容进行加密；跳过M_3位的内容，读取N_4字节的内容，从所生成的128位的密钥中获取0位的内容，则不对N_4字节的内容进行加密。加密过程结束。

在图2所示的实施例中，N_1、N_2、N_3和N_4是由与电子文档相关的信息确定的，N_1、N_2、N_3和N_4可以相等也可以不相等。

解密过程是加密过程的逆过程，这里不再赘述。

由上述可见，本发明这种当有用户请求下载指定数字文档时，生成密钥；对指定数字文档的内容进行分段加密，且每段内容加密所使用的密钥为所述生成密钥的一部分；用户所使用的客户端下载所述加密的数字文档后，根据所述密钥和对应的解密过程进行解密的技术方案，使得该加密方法不易被破解，增加了数字文档的安全性。

以上所述仅为本发明的较佳实例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明保护的范围之内。

权 利 要 求 书

1、一种加密方法，其特征在于，该方法包括：

当有用户请求下载指定数字文档时，实时生成密钥；

对指定数字文档的内容进行分段加密，且每段内容加密所使用的密钥为所述生成密钥的一部分；

用户所使用的客户端下载所述加密的数字文档后，根据所述密钥和对应的解密过程进行解密。

2、根据权利要求1所述的方法，其特征在于，所述对指定数字文档的内容进行分段加密，且每段内容加密所使用的密钥为所述生成密钥的一部分包括以下步骤：

A、跳过数字文档内容的文件头部分；令i＝1；

B、从所跳过的内容之后按顺序读取N_i字节的二进制内容，从所述生成密钥获取一定位数的内容作为本次密钥，用本次密钥对读取的二进制内容进行加密；

C、跳过M_i位的二进制内容；

D、判断对数字文档内容的加密是否完成，是则结束流程，否则令i＝i＋1，返回步骤B。

3、根据权利要求2所述的方法，其特征在于，

N_i由与所述指定数字文档相关的信息确定。

4、根据权利要求2所述的方法，其特征在于，

M_i等于所述指定数字文档的标识的位数。

5、根据权利要求2所述的方法，其特征在于，所述步骤B中的从所述生成密钥获取一定位数的内容作为本次密钥包括：

如果从所述生成密钥获取到零位的内容，则不对本次所读取的二进制内容进行加密。

6、根据权利要求3所述的方法，其特征在于，

所述与指定数字文档相关的信息包括：所述指定数字文档的固有信息的一种或多种。

说 明 书 附 图

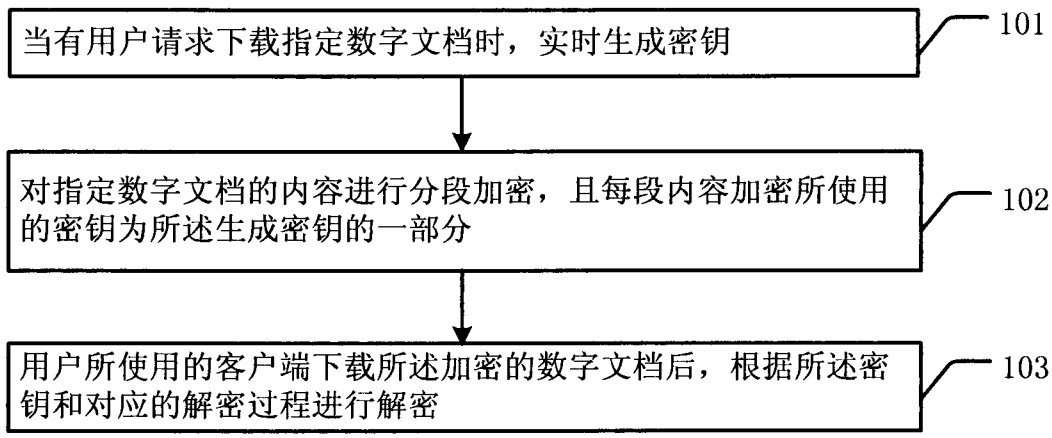
当有用户请求下载指定数字文档时，实时生成密钥
101
对指定数字文档的内容进行分段加密，且每段内容加密所使用的密钥为所述生成密钥的一部分
102
用户所使用的客户端下载所述加密的数字文档后，根据所述密钥和对应的解密过程进行解密
103

图 1

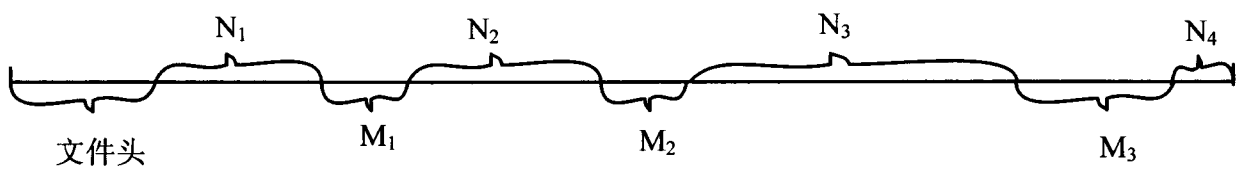
N1
N2
N3
N4
文件头
M1
M2
M3

图 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2011/001694

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/06 (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 9/-, H04L 29/-, G06F 21/-

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)

CPRSABS, CNKI: segment encryption download key division segmentation

DWPI: segment key encrypt+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E	CN 102377561 A (XIAMEN GEEBOO SCIENCE & TECHNOLOGY CO., LTD.), 14 March 2012 (14.03.2012), claims 1-6	1-6
L	CN 102402670 A (GUANG DONG OPPO MOBILE TELECOMMUNICATIONS CO., LTD.), 04. April 2012 (04.04.2012), description, paragraph 37 (Application date is earlier than the application date of the present application, publication date is later than the application date of the present application, and the content affects inventiveness)	1-6
Y	US 6490353 B1 (TAN), 03 December 2002 (03.12.2002), description, column 4, line 59 to column 5, line 22, and figure 1	1-6
Y	CN 102143175 A (BEIJING BENY WAVE SCIENCE & TECHNOLOGY CO., LTD.), 03 August 2011 (03.08.2011), claims 1 and 7	1-6

☐ 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
28 June 2012 (28.06.2012)	**12 July 2012 (12.07.2012)**
Name and mailing address of the ISA/CN: 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 **WANG, Zhiwei** Telephone No.: (86-10) **62411285**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2011/001694

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102377561 A	14.03.2012	None	
CN 102402670 A	04.04.2012	None	
US 6490353 B1	03.12.2002	WO 0031917 A1	02.06.2000
		AU 1702900 A	13.06.2000
CN 102143175 A	03.08.2011	None	

国际检索报告

国际申请号
PCT/CN2011/001694

A. 主题的分类

H04L 9/06 (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: H04L9/-,H04L29/-,G06F21/-

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）)

CPRSABS, CNKI: 段 加密 下载 密钥 部分 分段

DWPI: segment key encrypt+

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
E	CN102377561A （厦门简帛信息科技有限公司） 14. 3 月 2012（14.03.2012）权利要求 1-6	1-6
L	CN102402670 A （广东欧珀移动通信有限公司） 04. 4 月 2012（04.04.2012）说明书第 37 段（申请日比本申请的申请日早、公开日比本申请的申请日晚、内容影响创造性）	1-6
Y	US6490353B1 （Tan）03. 12 月 2002（03.12.2002） 说明书第 4 列第 59 行至第 5 列第 22 行，图 1	1-6
Y	CN102143175A （北京百纳威尔科技有限公司） 03. 8 月 2011（03.08.2011）权利要求 1、7	1-6

☐ 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
28. 6 月 2012（28.06.2012）	**12.7 月 2012 (12.07.2012)**
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 王志伟 电话号码：(86-10) 62411285

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2011/001694

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN102377561 A	14.03.2012	无	
CN102402670 A	04.04.2012	无	
US6490353B1	03.12.2002	WO0031917 A1	02.06.2000
		AU1702900 A	13.06.2000
CN102143175A	03.08.2011	无	