

(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  
2020 年 7 月 9 日 (09.07.2020)



(10) 国际公布号  
**WO 2020/140926 A1**

(51) 国际专利分类号:  
**H04L 9/08** (2006.01)

(21) 国际申请号: PCT/CN2020/070036

(22) 国际申请日: 2020 年 1 月 2 日 (02.01.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:  
201910000352.X 2019 年 1 月 2 日 (02.01.2019) CN

(71) 申请人: 中国移动通信有限公司研究院 (CHINA MOBILE COMMUNICATION CO., LTD RESEARCH INSTITUTE) [CN/CN]; 中国北京市西城区宣武门西大街 32 号, Beijing 100053 (CN)。  
中国移动通信集团有限公司 (CHINA MOBILE COMMUNICATIONS GROUP CO., LTD.) [CN/CN]; 中国北京市西城区金融大街 29 号, Beijing 100032 (CN)。

(72) 发明人: 刘福文 (LIU, Fuwen); 中国北京市西城区宣武门西大街 32 号, Beijing 100053 (CN)。

(74) 代理人: 北京派特恩知识产权代理有限公司 (CHINA PAT INTELLECTUAL PROPERTY OFFICE); 中国北京市海淀区海淀南路 21 号中关村知识产权大厦 B 座 2 层, 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, 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, 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, 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) 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, ST, 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,

(54) Title: KEY GENERATION METHOD, TERMINAL DEVICE AND NETWORK DEVICE

(54) 发明名称: 一种密钥生成方法、终端设备及网络设备

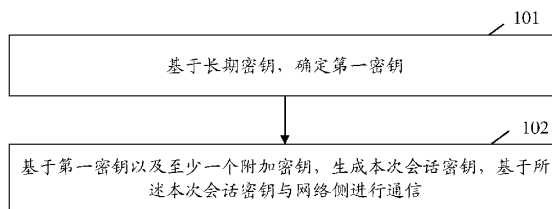


图 1

101 Determining a first key based on the long-term key  
102 Generating the session key based on the first key and at least one additional key, communicating with the network side based on the session key

(57) Abstract: The embodiment of the present application provides a key generation method, which relates to a terminal device, a network device and a computer-readable storage medium, wherein the method includes: determining a first key based on the long-term key; generating the session key based on the first key and at least one additional key, communicating with the network side based on the session key; wherein, the at least one additional key includes: an initial session key generated when the terminal device is connected to the network for the first time, and/or a session key used in the last communication; the first key and the at least one additional key are both symmetric keys.

(57) 摘要: 本申请实施例提供了一种密钥生成方法、其涉及终端设备、网络设备以及计算机可读存储介质, 其中方法包括: 基于长期密钥, 确定第一密钥; 基于第一密钥以及至少一个附加密钥, 生成本次会话密钥, 基于所述本次会话密钥与网络侧进行通信; 其中, 所述至少一个附加密钥中包括: 终端设备初次连接网络时生成的初始会话密钥, 和/或, 上一次通信使用的会话密钥; 所述第一密钥以及所述至少一个附加密钥均为对称密钥。

[见续页]

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)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。