(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
2022 年 2 月 10 日 (10.02.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/028289 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01) *G06F 21/60* (2013.01)

(21) 国际申请号: PCT/CN2021/108935

(22) 国际申请日: 2021 年 7 月 28 日 (28.07.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202010790159.3 2020年8月7日 (07.08.2020) CN

(71) 申请人: 百果园技术（新加坡）有限公司 (BIGO TECHNOLOGY PTE. LTD.) [SG/SG]; 新加坡巴西班让路枫树商业城 30 号楼 15 层 31A, Singapore 117440 (SG)。

(72) 发明人; 及

(71) 申请人 (仅对*US*): 李岩 (LI, Yan) [CN/CN]; 中国广东省广州市番禺区市桥街兴泰路274号C栋西塔5-13层, Guangdong 511402 (CN)。

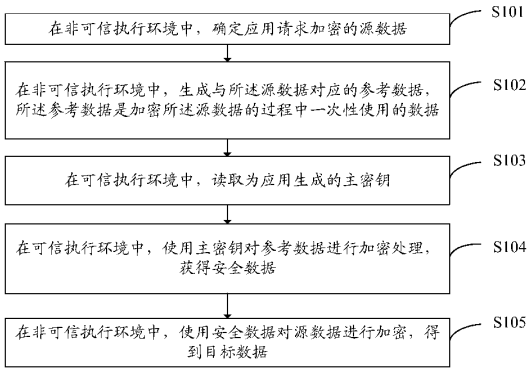
(74) 代理人: 北京品源专利代理有限公司 (BEYOND ATTORNEYS AT LAW); 中国北京市海淀区莲花池东路39号西金大厦6层, Beijing 100036 (CN)。

(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, IT, 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,

(54) **Title:** DATA ENCRYPTION METHOD AND APPARATUS, DATA DECRYPTION METHOD AND APPARATUS, TERMINAL, AND STORAGE MEDIUM

(54) **发明名称**: 数据加密方法、数据解密方法、装置、终端和存储介质



S101 In a non-trusted execution environment, determine source data requested to be encrypted by an application
S102 In the non-trusted execution environment, generate reference data corresponding to the source data, the reference data being one-time data in the process of encrypting the source data
S103 In a trusted execution environment, read a master key generated for the application
S104 In the trusted execution environment, encrypt the reference data by using the master key to obtain security data
S105 In the non-trusted execution environment, encrypt the source data by using the security data to obtain target data

图 1

(57) **Abstract:** Disclosed in embodiments of the present application are a data encryption method and apparatus, a data decryption method and apparatus, a terminal, and a storage medium. The data encryption method comprises: in a non-trusted execution environment, determining source data requested to be encrypted by an application; in the non-trusted execution environment, generating reference data corresponding to the source data; in a trusted execution environment, reading a master key generated for the application; in the trusted execution environment, encrypting the reference data by using the master key to obtain security data; and in the non-trusted execution environment, encrypting the source data by using the security data to obtain target data.

(57) **摘要**: 本申请实施例公开了一种数据加密方法、数据解密方法、装置、终端和存储介质，该数据加密方法包括：在非可信执行环境中，确定应用请求加密的源数据；在非可信执行环境中，生成与所述源数据对应的参考数据；在可信执行环境中，读取为应用生成的主密钥；在可信执行环境中，使用主密钥对参考数据进行加密处理，获得安全数据；在非可信执行环境中，使用所述安全数据对所述源数据进行加密，得到目标数据。

WO 2022/028289 A1

[见续页]

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, KM, ML, MR, NE, SN, TD, TG)。

根据细则4.17的声明:

- 关于申请人有权申请并被授予专利(细则4.17(ii))
- 关于申请人有权要求在先申请的优先权(细则4.17(iii))
- 发明人资格(细则4.17(iv))

本国际公布:

- 包括国际检索报告(条约第21条(3))。