

(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
2018 年 3 月 8 日 (08.03.2018)



(10) 国际公布号
WO 2018/040921 A1

(51) 国际专利分类号:
G06F 7/58 (2006.01)

(21) 国际申请号: PCT/CN2017/097779

(22) 国际申请日: 2017 年 8 月 17 日 (17.08.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610751289.X 2016年8月29日 (29.08.2016) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人: 张贺 (ZHANG, He); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (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,

(54) Title: RANDOM NUMBER GENERATION METHOD AND DEVICE UTILIZED IN COMPUTER SYSTEM

(54) 发明名称: 计算机系统中随机数的生成方法及装置

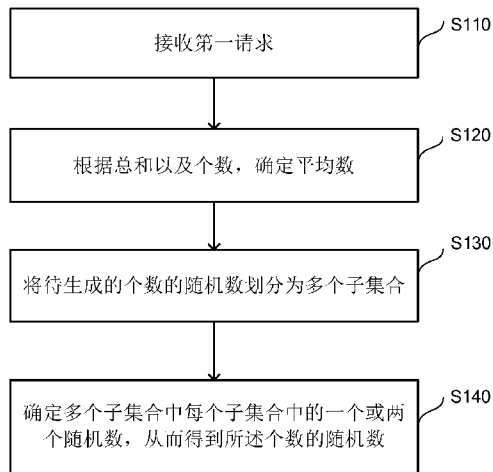


图 1

S110 Receive a first request
S120 Determine according to a sum and a number count, an average number
S130 Sort a specified number of the random numbers to be provided into a plurality of subsets
S140 Determine that each of the subsets contains one or two random numbers to obtain the specified number of random numbers

(57) Abstract: A random number generation method and device utilized in a computer system. In one embodiment, the random number generation method comprises: upon receiving a first request, sorting random numbers to be provided into a plurality of subsets, wherein when a subset contains two random numbers, a sum of the two random numbers is twice of an average number, and a quotient of the two random numbers is a preconfigured threshold value; and then sequentially determining that each of the subsets contains one or two random numbers to obtain a specified number of random numbers. As a result, the embodiment achieves the goal of controlling random number generation.

PT, QA, RO, RS, RU, RW, SA, 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, 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,
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))。

(57) 摘要: 一种计算机系统中随机数的生成方法及装置, 在一种计算机系统中随机数的生成方法中, 在接收到第一请求时, 首先将待生成的随机数划分为多个子集合, 并在子集合包括两个随机数时, 规定两个随机数之和为平均数的两倍, 两个随机数之商为预设阈值; 之后再依次确定各个子集合中包括的一个或两个随机数, 从而得到指定个数的随机数; 由此实现了对生成的随机数进行控制的目的。

计算机系统中随机数的生成方法及装置

本申请要求 2016 年 08 月 29 日递交的申请号为 201610751289.X、发明名称为“计算机系统中随机数的生成方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本申请涉及计算机技术领域，尤其涉及一种计算机系统中随机数的生成方法及装置。

背景技术

10 传统技术中，在生成指定个数的随机数时，往往通过调用随机函数来随机生成该指定个数的随机数，然而因为上述随机数是随机生成的，所以无法对其进行有效的控制（如，控制在某一范围内），由此会导致生成的指定个数的随机数分布不均匀的问题。比如，在实现“红包”的发送的场景中，支付服务端随机生成的“红包金额”可能会非常大，也可能会非常小（如，0.01），这会给用户带来较差的体验。

15

发明内容

本申请描述了一种计算机系统中随机数的生成方法及装置，可以实现对生成的随机数进行有效的控制。

第一方面，提供了一种计算机系统中随机数的生成方法，该方法包括：

20 接收第一请求，所述第一请求包括待生成的随机数的总和以及个数；

根据所述总和以及所述个数，确定平均数；

将待生成的所述个数的随机数划分为多个子集合，其中，每个子集合包括一个或两个随机数，当子集合包括两个随机数时，所述两个随机数之和为所述平均数的两倍，且所述两个随机数之商为预设阈值；

25 确定所述多个子集合中每个子集合中的一个或两个随机数，从而得到所述个数的随机数。

第二方面，提供了一种计算机系统中随机数的生成装置，该装置包括：

接收单元，用于接收第一请求，所述第一请求包括待生成的随机数的总和以及个数；

确定单元，用于根据所述接收单元接收的所述总和以及所述个数，确定平均数；

30 划分单元，用于将待生成的所述个数的随机数划分为多个子集合，其中，每个子集

合包括一个或两个随机数，当子集合包括两个随机数时，所述两个随机数之和为所述平均数的两倍，且所述两个随机数之商为预设阈值；

所述确定单元，还用于确定所述多个子集合中每个子集合中的一个或两个随机数，从而得到所述个数的随机数。

- 5 本申请提供的计算机系统中随机数的生成方法及装置，在接收到第一请求时，首先将待生成的随机数划分为多个子集合，并在子集合包括两个随机数时，规定两个随机数之和为平均数的两倍，两个随机数之商为预设阈值；之后再依次确定各个子集合中包括的一个或两个随机数，从而得到指定个数的随机数；由此实现了对生成的随机数进行控制的目的。

10

附图说明

为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其

15 它的附图。

图 1 为本申请一种实施例提供的计算机系统中随机数的生成方法流程图；

图 2 为本申请提供的子集合中随机数的确定方法流程图；

图 3 为本申请提供的计算机系统中随机数的生成方法的一种应用场景的示意图；

图 4 为图 3 所示的场景中一种红包金额的生成方法流程图；

- 20 图 5 为图 3 所示的场景中另一种红包金额的生成方法流程图；

图 6 为本申请一种实施例提供的计算机系统中随机数的生成装置示意图。

具体实施方式

下面结合附图，对本发明的实施例进行描述。

- 25 本申请提供的计算机系统中随机数的生成方法及装置适用于在待生成的随机数的总和以及个数固定的情况下，生成随机数的场景；尤其适用于在待生成的随机数的总和以及个数固定的情况下，生成分布均匀的随机数的场景。

图 1 为本申请一种实施例提供的计算系统中随机数的生成方法流程图。所述方法的执行主体可以为具有处理能力的设备：服务器或者系统或者装置，如，支付系统的服务端，如图 1 所示，所述方法具体可以包括：

30

步骤 110, 接收第一请求。

其中, 该第一请求可以为任一用于指示上述服务器或者系统或者装置生成随机数的请求。该第一请求中可以包括待生成的随机数的总和以及待生成的随机数的个数等。

步骤 120, 根据总和以及个数, 确定平均数。

5 此处, 平均数可以为总和除以个数得到的商。以“红包”发送的场景为例来说, 假设红包总金额为 100 元, 红包数量为 10 个, 则平均分配金额可以为 $100/10=10$ 元, 也即平均每个人可以分配 10 元。

步骤 130, 将待生成的个数的随机数划分为多个子集合。

10 其中, 每个子集合包括一个或两个随机数, 当子集合包括两个随机数时, 两个随机数之和为平均数的两倍, 且两个随机数之商为预设阈值。

此处, 子集合的数量可以根据待生成的随机数的个数确定, 如, 子集合的数量可以根据如下公式计算: $\text{INT}(\text{个数}/2)$ 或者 $\text{INT}(\text{个数}/2) + 1$, 其中, $\text{INT}()$ 是取整函数, 即其用于获取一个数据的整数部分, 具体地, 当待生成的随机数的个数为偶数时, 可以根据公式: $\text{INT}(\text{个数}/2)$, 确定子集合的数量; 而当待生成的随机数的个数为奇数时, 15 可以根据公式 $\text{INT}(\text{个数}/2) + 1$, 确定子集合的数量。可以理解的是, 在上述待生成的随机数的个数为偶数的情况下, 各子集合中可以都包括两个随机数; 而在待生成的随机数的个数为奇数的情况下, 则至少有一个子集合只包括一个随机数。

举例来说, 假设待生成的随机数的个数为 10 个, 也即待生成的随机数的个数为偶数, 因此可以确定子集合的数量为: $\text{INT}(10/2) = 5$ 个。对划分得到的 5 个子集合, 当每个 20 子集合均包括两个随机数时, 可以规定该两个随机数的和为平均数的两倍, 且该两个随机数的商为预设阈值, 在对两个随机数作出上述规定之后, 该两个随机数就可以构成如下二元一次方程:

$$\begin{cases} S_1 + S_2 = 2AVG \\ S_1 / S_2 = GAP \end{cases} \quad (\text{公式 1})$$

25 其中, S_1 和 S_2 分别表示子集合中的两个随机数, AVG 为上述平均数, 而 GAP 是指上述预设阈值, 其可以根据实际需求确定。

在再一个例子中, 假设待生成的随机数的个数为 9 个, 也即待生成的随机数的个数为奇数时, 可以确定子集合的数量为: $\text{INT}(9/2) + 1 = 5$ 个。对划分得到的 5 个子集合, 当 1 个子集合包括 1 个随机数, 而其它子集合包括两个随机数时, 也可以规定该两个随

机数的和为平均数的两倍，且该两个随机数的商为预设阈值，在对两个随机数作出上述规定之后，该两个随机数也可以构成如上公式 1 所示的二元一次方程。

需要说明的是，本申请中，通过将子集合中两个随机数的和与商进行相应的规定，可以实现对同一子集合中两个随机数的差距进行控制的目的，且各随机数在中间区域相对平均，也即各随机数是在以平均数为中心划分出的范围之内，由此可以保证生成的随机数分布比较均匀。

步骤 140，确定多个子集合中每个子集合中的一个或两个随机数，从而得到所述个数的随机数。

在待生成的随机数的个数为偶数的情况下，根据公式 1 可以确定出每个子集合中的两个随机数；在确定出每个子集合中的两个随机数之后，就可以得到所述个数的随机数；如前述例子，在确定出 5 个子集合中的每个随机数之后，就可以得到 10 个随机数。需要说明的是，当某一子集合中包括 1 个随机数时，则该一个随机数可以根据平均数数确定，如，可以将平均数随机衰减后作为上述一个随机数，或者，也可以通过其它方式确定，如，直接将平均数作为上述一个随机数，本申请对此不作限定。

需要说明的是，对于子集合中包括两个随机数的情况，上述只是给出了子集合中两个随机数的一种确定方法，在本申请的其它实施方式中，子集合中的两个随机数也可以通过如图 2 所示的各步骤确定：

步骤 210，根据待生成的随机数的个数，确定循环周期。

在一种实现方式中，可以根据公式 2 确定循环周期。

$$Interval = count / 2 \quad (\text{公式 2})$$

其中，Interval 为循环周期，count 为待生成的随机数的个数。

步骤 220，根据预设阈值，确定分配因子。

在一种实现方式中，可以根据公式 3 确定分配因子。

$$primer = (2 * GAP) / (1 + GAP) \quad (\text{公式 3})$$

其中，primer 为分配因子，GAP 为预设阈值。

步骤 230，根据平均数以及分配因子，确定最大相差倍数。

在一种实现方式中，可以根据公式 4 确定最大相差倍数。

$$top = \text{Math.min}((AVG * primer), (2 * AVG - 1)) \quad (\text{公式 4})$$

其中，top 为最大相差倍数，AVG 为平均数，primer 为分配因子，Math.min()为取最

小值函数，如，其会比较（AVG*primer）与（2*AVG-1）两个数的大小，然后取最小的数作为最大相差倍数。

步骤 240，根据最大相差倍数、平均数以及循环周期，确定步差。

在一种实现方式中，可以根据公式 5 确定步差。

$$5 \quad \text{stepM} = (\text{top} - \text{AVG}) / \text{Interval} \quad (\text{公式 5})$$

其中，stepM 为步差，top 为最大相差倍数，AVG 为平均数，Interval 为循环周期。

步骤 250，根据步差，确定随机数的偏移范围。

在一种实现方式中，可以根据公式 6 确定随机数的偏移范围。

$$Ri = (\text{int})(1d / (5 + \text{random.nextInt}(25))) * \text{stepM} \quad (\text{公式 6})$$

10 其中，Ri 为偏移范围，stepM 为步差，random.nextInt(25) 为随机选取 0-25 之间任一整数的随机函数，根据公式 6 可以确定 Ri 为 [0, 1/30*stepM]，也即偏移范围为 [0, 1/30*stepM]。

步骤 260，确定在偏移范围内的第一偏移量。

此处的第一偏移量可以是指从偏移范围 [0, 1/30*stepM] 内随机选取的任一值。

15 步骤 270，根据最大相差倍数、步差、当前步长以及第一偏移量，确定两个随机数中的第一随机数。

在一种实现方式中，可以根据公式 7 确定两个随机数中的第一随机数。

$$S_1 = \text{top} - (\text{int})((\text{stepGo}++) * \text{stepM}) - ri \quad (\text{公式 7})$$

20 其中，S₁ 为两个随机数中的第一随机数，该第一随机数可以是指两个随机数中较大的随机数；top 为最大相差倍数；stepGo 为当前步长，当确定第一个子集合中的第一随机数时，stepGo 可以为 0，之后，当确定第二个子集合中的第一随机数时，stepGo 可以为 1，即每次递增 1，这样依次类推；stepM 为步差；ri 为第一偏移量。

步骤 280，根据平均数以及第一随机数，确定两个随机数中的第二随机数。

在一种实现方式中，可以根据公式 8 确定两个随机数中的第二随机数。

$$25 \quad S_2 = (\text{int})(2 * \text{AVG}) - S_1 \quad (\text{公式 8})$$

其中，S₂ 为两个随机数中的第二随机数，该第二随机数可以是指两个随机数中较小的随机数；AVG 为平均数；S₁ 为两个随机数中的第一随机数。

上述是在其它实施方式中，子集合中两个随机数的确定方法，而当子集合只包括一个随机数时，则该一个随机数可以通过如下步骤确定：

对平均数进行随机衰减；

根据随机衰减后的平均数以及预设的最小随机数，确定第二子集合中的一个随机数。

此处的第二子集合可以是指任一只包括一个随机数的子集合。

在一种实现方式中，可以根据公式 9 确定第二子集合中的一个随机数。

5
$$S_1 = (\text{int}) \text{Math.max}(\text{MIN}, (\text{AVG} - 1 - \text{random.nextInt}(\text{FLUCTUATION}))) \quad (\text{公式 9})$$

其中， S_1 为第二子集合中的一个随机数；MIN 为预设的最小随机数，如，可以为 0.01；AVG 为平均数；FLUCTUATION 可以为预先设定的常量，该常量可以为想要对平均数衰减的值；Math.max() 为取最大值函数，如，其会比较 MIN 与 $(\text{AVG} - 1 - \text{random.nextInt}(\text{FLUCTUATION}))$ 两个数的大小，然后取最大的数作为第二子集合中的一个随机数。

回到步骤 140 中，可以理解的是，在依照一个子集合中一个或者两个随机数的确定方法（如，图 2 中的各步骤），确定出每个子集合中的一个或者两个随机数之后，就可以得到所述个数的随机数。

可选地，在执行步骤 140 之后，还可以执行如下步骤：

15 步骤 A：根据总和以及所述个数的随机数，确定剩余数。

需要说明的是，根据传统的方法或者图 2 中的各步骤得到的所述个数的随机数之和往往并不等于总和。如在“红包”发送的场景中，红包数量的红包金额之和，也即发送的“红包”的金额之和往往并不等于红包总金额，由此就造成了资金亏损的问题。为解决该问题，本申请中，可以根据总和以及所述个数的随机数，确定剩余数，如，可以通过计算总和与所述个数的随机数之和的差值，来确定剩余数。如前述例子，在红包总金额为 100 元的情况下，假设 10 个红包金额之和为 90 元，则剩余金额为 10 元。

当然，在实际应用中，剩余数也可以在执行图 2 各步骤的时候确定，由此，可以提高剩余数的确定效率。在一个例子中，可以将剩余数初始化为总和，之后，在每次确定出一个子集合中的一个或者两个随机数之后，就将剩余数更新为剩余数与一个随机数的差值，或者将剩余数更新为剩余数与两个随机数之和的差值，可以理解的是，当所有的子集合中的随机数确定完成之后，更新后的剩余数即为最终的剩余数。

步骤 B：对剩余数进行拆分。

在一种实现方式中，可以将剩余数拆分为所述个数的子数据。如前述例子，在剩余金额为 10 元，而红包数量为 10 个时，拆分后得到的子数据可以为 10 个 1 元。当然，在

实际应用中，也可以将剩余数拆分为其它个数的子数据，且各子数据可以不相同，本申请对此不作限定。

步骤 C：将拆分后的剩余数叠加至所述个数的随机数中，得到更新后的所述个数的随机数。

- 5 举例来说，假设总和：10，待生成的随机数的个数为 10 个，得到的 10 个随机数分别为：1.2、0.7、1.1、0.8、1.3、0.6、1.5、0.4、1.0 和 0.9，则剩余数可以为：0.5；将剩余数 0.5 拆分为 10 个 0.05；则更新后的 10 个随机数可以为：1.25、0.75、1.15、0.85、1.35、0.65、1.55、0.45、1.05 和 0.95。

- 10 在“红包”发送的场景下，通过将拆分后的剩余金额叠加至红包数量的红包金额中，可以避免资金损失。

可选地，在执行步骤 140 之后，或者在执行步骤 C 之后，还可以执行如下步骤：

步骤 X：对所述个数的随机数进行重排序。

- 15 此处，可以是按照任意的顺序对所述个数的随机数进行重排序，以避免各随机数按大小顺序存储；此外，还可以保证在待生成的随机数的总和以及个数相同的情况下，连续两次以上划分的所述个数的随机数的顺序不一致。

步骤 Y：将重排序后的所述个数的随机数存储到列表中。

当然，在实际用中，也可以将重排序后的所述个数的随机数数存储到其它形式的存储单元中，本申请对此不作限定。

- 20 需要说明的是，上述步骤 X 和步骤 Y 中的所述个数的随机数也可以是指叠加了拆分后的剩余数的所述个数的随机数。

- 需要说明的是，本申请提供的计算机系统中随机数的生成方法可以应用于如图 3 所示的“红包”的发送的场景，图 3 中，包括一个发送方客户端以及多个接收方客户端，发送方客户端用于发送“红包”领取通知，接收方客户端用于根据发送方客户端发送的“红包”领取通知，执行相应的“红包”领取操作。需要说明的是，发送方客户端发送“红包”领取通知的方式有多种，以发送方客户端为支付宝客户端为例来说，支付宝客户端发送“红包”领取通知的方式可以包括两种：第一种，支付宝客户端可以在群组中发送“红包”领取通知，该群组可以通过以下步骤建立：通讯录->群聊->选择群类型（如，娱乐群）->选择用户；第二种，发送方用户在“支付宝”应用界面中，通过触发“红包”文字或相应的“红包”图案，即可转入红包生成界面；在红包生成界面，发送方用户输入口令，并在选择的群类型中输入“总金额”以及“红包个数”，之后点击“发红包”
- 25
- 30

后，即可完成“红包”领取通知的发送。可以理解的是，通过上述两种方式发送的“红包”领取通知可以包括“总金额”和“红包个数”等信息。

图 3 中，在发送方客户端发送“红包”领取通知之后，服务端就可以接收到第一请求，该第一请求中可以包括红包总金额以及待发送的红包数量，之后服务端可以从红包总金额中划分出红包数量的红包金额；当服务端接收到接收方客户端发送的“红包”领取请求时，也即在接收方用户领取红包时，将其中的一个红包金额分配给接收方客户端。

然而，在服务端划分红包数量的红包金额的过程中，通常随机生成每个红包金额，由此服务端随机生成的红包金额可能会非常大，也可能会非常小（如，0.01），也即具有红包金额不可控的问题。

当本申请的计算机系统中随机数的生成方法应用于图 3 所示的场景中时，可以解决上述红包金额不可控的问题。具体地，当本申请的计算机系统中随机数的生成方法应用于图 3 所示的场景中时，待生成的随机数的总和相当于红包总金额，待生成的随机数的个数相当于待发送的红包数量，随机数相当于红包金额，而随机数的生成方法可以为红包金额的生成方法，其中，图 4 提供了一种红包金额的生成方法，图 4 中，该方法具体可以包括如下步骤：

步骤 410，服务端接收发送方客户端发送的第一请求。

该第一请求可以包括红包总金额以及待发送的红包数量。

步骤 420，根据红包总金额和红包数量，确定平均分配金额。

此处，平均分配金额可以为红包总金额除以红包数量得到的商。举例来说，假设红包总金额为 100 元，红包数量为 10 个，则平均分配金额可以为 $100/10=10$ 元，也即平均每个人可以分配 10 元。

步骤 430，将待生成的红包数量的红包金额划分为多个红包金额子集合。

其中，每个红包金额子集合包括一个或两个红包金额，当红包金额子集合包括两个红包金额时，两个红包金额之和为平均分配金额的两倍，且两个红包金额之商为预设阈值。

此处，红包金额子集合的数量可以根据待发送的红包数量确定，如，红包金额子集合的数量可以根据如下公式计算： $\text{INT}(\text{红包数量}/2)$ 或者 $\text{INT}(\text{红包数量}/2)+1$ ，其中， $\text{INT}()$ 是取整函数，即其用于获取一个数据的整数部分，具体地，当红包数量为偶数时，可以根据公式： $\text{INT}(\text{红包数量}/2)$ ，确定红包金额子集合的数量；而当红包数量为奇数时，可以根据公式 $\text{INT}(\text{红包数量}/2)+1$ ，确定红包金额子集合的数量。可以理解

的是，在上述红包数量为偶数的情况下，各红包金额子集合中可以都包括两个红包金额；而在红包数量为奇数的情况下，则至少有一个红包金额子集合只包括一个红包金额。

假设待发送的红包数量为 10 个，也即红包数量为偶数，因此可以确定红包金额子集合的数量为： $\text{INT}(10/2) = 5$ 个。对划分得到的 5 个红包金额子集合，当每个红包金额子集合均包括两个红包金额时，可以规定该两个红包金额的和为平均分配金额的两倍，且该两个红包金额的商为预设阈值，在对两个红包金额作出上述规定之后，该两个红包金额就可以构成如公式 1 所示的二元一次方程。

而假设待发送的红包数量为 9 个，也即红包数量为奇数时，可以确定红包金额子集合的数量为： $\text{INT}(9/2) + 1 = 5$ 个。对划分得到的 5 个红包金额子集合，当 1 个红包金额子集合包括 1 个红包金额，而其它红包金额子集合包括两个红包金额时，也可以规定该两个红包金额的和为平均分配金额的两倍，且该两个红包金额的商为预设阈值，在对两个红包金额作出上述规定之后，该两个红包金额也可以构成如上公式 1 所示的二元一次方程。

需要说明的是，本申请中，通过将红包金额子集合中两个红包金额的和与商进行相应的规定，可以实现对同一红包金额子集合中两个红包金额的差值进行控制的目的，且各红包金额在中间区域相对平均，也即各红包金额是在以平均分配金额为中心划分出的范围之内，由此可以保证各接收方客户端分配的红包金额相对平均，也即可以保证接收方用户分配的“红包”金额相对平均，这可以提升用户的体验。

步骤 440，确定多个红包金额子集合中每个红包金额子集合中的一个或两个红包金额，从而得到红包数量的红包金额。

在红包数量为偶数的情况下，根据公式 1 可以确定出每个红包金额子集合中的两个红包金额；在确定出每个红包金额子集合中的两个红包金额之后，就可以得到红包数量的红包金额；如前述例子，在确定出 5 个红包金额子集合中的每个红包金额之后，就可以得到 10 个红包金额。需要说明的是，当某一红包金额子集合中包括 1 个红包金额时，则该一个红包金额可以根据平均分配金额确定，如，可以将平均分配金额随机衰减后作为上述一个红包金额。此处，在红包数量为奇数的情况下，通过将平均分配金额随机衰减后赋予最后一个红包金额，可以避免最后一个红包金额固定的问题，由此可以避免不法分子利用这种规律进行不法行为的问题。

需要说明的是，对于红包金额子集合中包括两个红包金额的情况，上述只是给出了两个红包金额的一种确定方法，在本申请的其它实施方式中，红包金额子集合中的两个

红包金额也可以通过如图 2 所示的各步骤确定；即只需将图 2 所示的各步骤中的平均数替换为平均分配金额，将随机数替换为红包金额即可。

服务端在依照一个红包金额子集合中一个或者两个红包金额的确定方法（如，图 2 中的各步骤），确定出每个红包金额子集合中的一个或者两个红包金额之后，就可以得到红包数量的红包金额。

可选地，在执行步骤 440 之后，还可以执行如下步骤：

步骤 a：根据红包总金额以及红包数量的红包金额，确定剩余金额。

红包数量的红包金额之和，也即发送的“红包”的金额之和往往并不等于红包总金额，由此就造成了资金亏损的问题。为解决该问题，本申请中，可以根据红包总金额以及红包数量的红包金额，确定剩余金额，如，可以通过计算红包总金额与红包数量的红包金额之和的差值，来确定剩余金额。如前述例子，在红包总金额为 100 元的情况下，假设 10 个红包金额之和为 90 元，则剩余金额为 10 元。

当然，在实际应用中，剩余金额也可以在执行图 2 各步骤的时候确定，由此，可以提高剩余金额的确定效率。在一个例子中，可以剩余金额初始化为红包总金额，之后，在每次确定出一个红包金额子集合中的一个或者两个红包金额之后，就将剩余金额更新为剩余金额与一个红包金额的差值，或者将剩余金额更新为剩余金额与两个红包金额之后的差值，可以理解的是，当所有的红包金额子集合中的红包金额确定完成之后，更新后的剩余金额即为最终的剩余金额。

步骤 b：对剩余金额进行拆分。

在一种实现方式中，可以将剩余金额拆分为红包数量的子数据。如前述例子，在剩余金额为 10 元，而红包数量为 10 个时，拆分后得到的子数据可以为 10 个 1 元。当然，在实际应用中，也可以将剩余金额拆分为其它个数的子数据，且各子数据可以不相同，本申请对此不作限定。

步骤 c：将拆分后的剩余金额叠加至红包数量的红包金额中，得到更新后的红包数量的红包金额。

举例来说，假设红包总金额为：10 元，红包数量为 10 个，得到的 10 个红包金额分别为：1.2、0.7、1.1、0.8、1.3、0.6、1.5、0.4、1.0 和 0.9，则剩余金额可以为：0.5；将剩余金额 0.5 拆分为 10 个 0.05；则更新后的 10 个红包金额可以为：1.25、0.75、1.15、0.85、1.35、0.65、1.55、0.45、1.05 和 0.95。

通过将拆分后的剩余金额叠加至红包数量的红包金额中，可以避免资金损失。

可选地，在执行步骤 440 之后，或者在执行步骤 C 之后，还可以执行如下步骤：

步骤 x：对红包数量的红包金额进行重排序。

此处，可以是按照任意的顺序对红包数量的红包金额进行重排序，以避免各红包金额按大小顺序存储；此外，还可以保证在红包总金额和红包数量相同的情况下，连续两次以上划分的红包数量的红包金额的顺序不一致。

步骤 y：将重排序后的红包数量的红包金额存储到列表中。

当然，在实际用中，也可以将重排序后的红包数量的红包金额存储到其它形式的存储单元中，本申请对此不作限定。

需要说明的是，上述步骤 x 和步骤 y 中的红包数量的红包金额也可以是指更新后的红包数量的红包金额。

步骤 450，接收接收方客户端发送的第二请求。

该第二请求可以包括接收方用户的标识（例如，接收方用户的账号信息等）。

步骤 460，根据第二请求，将红包数量的红包金额中目标金额分配至接收方客户端。

此处的目标金额可以是指红包数量的红包金额中的任一红包金额，或者也可以是指更新后的红包数量的红包金额中任一红包金额。

如，服务端在接收到第二请求之后，可以从列表中读取目标金额；之后将目标金额分配至接收方客户端。

为了更清楚的说明本申请提供的计算机系统中随机数的生成方法在图 3 所示的“红包”的发送的场景中的应用，本申请给出了如下具体的实施方式。

图 5 为图 3 所示的场景中另一种红包金额的生成方法流程图。如图 5 所示，所述方法具体可以包括：

步骤 510，接收发送方客户端发送的第一请求。

可选地，在接收第一请求之前，可以预先设定最小分配金额（如，0.01 元）。

该第一请求可以包括红包总金额以及红包数量（count）。

步骤 520，判断红包数量（count）是否为 1，若是，则执行步骤 530；若否，则执行步骤 540。

步骤 530，将红包总金额放入列表。

步骤 540，判断红包总金额是否为红包数量*预设的最小分配金额，若是，则执行步骤 550；若否，则执行步骤 560。

步骤 550，采用平均分配算法将红包总金额划分为红包数量的最小分配金额，并将

其放入列表。

步骤 560, 计算平均分配金额、最大相差倍数、步差以及红包金额的偏移范围, 并将剩余金额初始化为红包总金额。

此处, 平均分配金额的计算方法可参照步骤 120 或者 420, 最大相差倍数、步差以及红包金额的偏移范围可以参照步骤 210-步骤 250, 在此不复赘述。

步骤 570, 判断是否已确定出红包数量的红包金额, 若否, 则执行步骤 580, 若是, 则执行步骤 5160。

步骤 580, 判断当前确定的红包金额是否是最后一个红包金额, 若是, 则执行步骤 590; 若否, 则执行步骤 5120。

10 步骤 590, 对平均分配金额进行随机衰减。

步骤 5100, 根据随机衰减后的平均分配金额以及预设的最小分配金额, 确定最后一个红包金额。

步骤 5110, 将最后一个红包金额加入列表中, 并将剩余金额更新为剩余金额与最后一个红包金额的差值。

15 步骤 5120, 从步骤 560 中计算的偏移范围之内随机选取任一值作为当前的偏移量。

步骤 5130, 根据步骤 560 中计算的最大相差倍数、步差、第一偏移量以及当前步长, 计算出一个红包金额。

此处, 一个红包金额的计算方法可以参照步骤 370。

步骤 5140, 根据平均分配金额以及一个红包金额, 计算另一红包金额。

20 此处, 另一红包金额的计算方法可以参照步骤 380。

步骤 5150, 将剩余金额更新为剩余金额与上述两个红包金额之和的差值, 并将一个红包金额与另一红包金额加入列表。

步骤 5160, 判断剩余金额是否大于 0, 若是, 则执行步骤 5170; 若否, 则执行步骤 5180。

25 步骤 5170, 对剩余金额进行拆分; 将拆分后的剩余金额叠加至红包数量的红包金额中, 得到更新后的红包数量的红包金额。

此处, 剩余金额的拆分方法以及叠加拆分后的剩余金额的方法可以参照步骤 B-步骤 C 或者步骤 b-步骤 c。

步骤 5180, 将红包数量的红包金额或者更新后的红包数量的红包金额进行重排序。

30 步骤 5190, 接收接收方客户端发送的第二请求。

步骤 5200, 将红包数量的红包金额或者更新后的红包数量的红包金额中的目标金额分配至接收方客户端。

本申请的上述实施例具有如下技术效果:

1) 通过对红包金额子集合中两个红包金额的和与商的限定, 可以实现对划分的红包
5 金额的控制。

2) 通过对剩余金额进行拆分, 并将拆分后的剩余金额叠加至红包数量的红包金额中, 可以保障不会出现资损; 此外, 还可以保障分配更均匀。

3) 通过对红包数量的红包金额进行重排序, 可以避免红包数量的红包金额按大小顺序存储。

10 4) 在红包数量为奇数的情况下, 通过将平均分配金额随机衰减后赋予最后一个红包金额, 可以避免最后一个红包金额固定的问题, 由此可以避免不法分子利用这种规律进行不法行为的问题。

当然, 本申请提出的计算机系统中随机数的生成方法并不局限于“红包”发送的场景, 也可以应用于其它的场景, 如商户活动金额分配, 本申请对此不作限定。

15 与上述计算机系统中随机数的生成方法对应地, 本申请实施例还提供的一种计算机系统中随机数的生成装置, 如图 6 所示, 该装置包括:

接收单元 601, 用于接收第一请求, 该第一请求包括待生成的随机数的总和以及个数。

确定单元 602, 用于根据接收单元 601 接收的总和以及个数, 确定平均数。

20 划分单元 603, 用于将待生成的个数的随机数划分为多个子集合, 其中, 每个子集合包括一个或两个随机数, 当子集合包括两个随机数时, 两个随机数之和为平均数的两倍, 且两个随机数之商为预设阈值。

确定单元 602, 还用于确定多个子集合中每个子集合中的一个或两个随机数, 从而得到所述个数的随机数。

25 可选地, 确定单元 602, 还用于根据个数, 确定循环周期;

根据预设阈值, 确定分配因子;

根据平均数以及分配因子, 确定最大相差倍数;

根据最大相差倍数、平均数以及循环周期, 确定步差;

根据步差, 确定随机数的偏移范围;

30 确定单元 602 具体用于:

确定在偏移范围内的第一偏移量；

根据最大相差倍数、步差、当前步长以及第一偏移量，确定两个随机数中的第一随机数；

根据平均数以及第一随机数，确定两个随机数中的第二随机数。

5 可选地，确定单元 602，还用于对平均数进行随机衰减；

根据随机衰减后的平均数以及预设的最小随机数，确定第二子集合中的一个随机数。

可选地，所述装置还包括：拆分单元 603 和叠加单元 604。

确定单元 602，还用于根据总和以及所述个数的随机数，确定剩余数；

拆分单元 603，用于对确定单元 602 确定的剩余数进行拆分；

10 叠加单元 604，用于将拆分单元 603 拆分后的剩余数叠加至所述个数的随机数中，得到更新后的所述个数的随机数。

可选地，所述装置还包括：

排序单元 605，用于对所述个数的随机数进行重排序；

存储单元 606，用于将排序单元 605 重排序后的所述个数的随机数存储到列表中。

15 本申请实施例装置的各功能模块的功能，可以通过上述方法实施例的各步骤来实现，因此，本申请提供的装置的具体工作过程，在此不复赘述。

本申请实施例提供的计算机系统中随机数的生成装置，接收单元 601 接收第一请求，该第一请求包括待生成的随机数的总和以及个数；确定单元 602 根据总和以及个数，确定平均数；划分单元 603 将待生成的个数的随机数划分为多个子集合；确定单元 602 确定多个子集合中每个子集合中的一个或两个随机数，从而得到所述个数的随机数。由此实现了对生成的随机数进行控制的目的。

20

本领域技术人员应该可以意识到，在上述一个或多个示例中，本发明所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。

25

以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本发明的保护范围之内。

权利要求书

1.一种计算机系统中随机数的生成方法，其特征在于，该方法包括：

接收第一请求，所述第一请求包括待生成的随机数的总和以及个数；

根据所述总和以及所述个数，确定平均数；

- 5 将待生成的所述个数的随机数划分为多个子集合，其中，每个子集合包括一个或两个随机数，当子集合包括两个随机数时，所述两个随机数之和为所述平均数的两倍，且所述两个随机数之商为预设阈值；

确定所述多个子集合中每个子集合中的一个或两个随机数，从而得到所述个数的随机数。

- 10 2.根据权利要求1所述的方法，其特征在于，当所述多个子集合中的第一子集合包括两个随机数时，在确定所述第一子集合中的两个随机数之前，所述方法还包括：

根据所述个数，确定循环周期；

根据所述预设阈值，确定分配因子；

根据所述平均数以及所述分配因子，确定最大相差倍数；

- 15 根据所述最大相差倍数、所述平均数以及所述循环周期，确定步差；

根据所述步差，确定随机数的偏移范围；

所述确定所述第一子集合中的两个随机数，包括：

确定在所述偏移范围内的第一偏移量；

根据所述最大相差倍数、所述步差、当前步长以及所述第一偏移量，确定所述两个

- 20 随机数中的第一随机数；

根据所述平均数以及所述第一随机数，确定所述两个随机数中的第二随机数。

3.根据权利要求1所述的方法，其特征在于，当所述多个子集合中的第二子集合包括一个随机数时，所述确定所述第二子集合中的一个随机数，包括：

对所述平均数进行随机衰减；

- 25 根据随机衰减后的平均数以及预设的最小随机数，确定所述第二子集合中的一个随机数。

4.根据权利要求1-3任一项所述的方法，其特征在于，所述方法还包括：

根据所述总和以及所述个数的随机数，确定剩余数；

对所述剩余数进行拆分；

- 30 将拆分后的剩余数叠加至所述个数的随机数中，得到更新后的所述个数的随机数。

5.根据权利要求 1-4 任一项所述的方法，其特征在于，在所述得到所述个数的随机数之后，所述方法还包括：

对所述个数的随机数进行重排序；

将重排序后的所述个数的随机数存储到列表中。

5 6.一种计算机系统中随机数的生成装置，其特征在于，该装置包括：

接收单元，用于接收第一请求，所述第一请求包括待生成的随机数的总和以及个数；

确定单元，用于根据所述接收单元接收的所述总和以及所述个数，确定平均数；

划分单元，用于将待生成的所述个数的随机数划分为多个子集合，其中，每个子集合包括一个或两个随机数，当子集合包括两个随机数时，所述两个随机数之和为所述平均数的两倍，且所述两个随机数之商为预设阈值；

10

所述确定单元，还用于确定所述多个子集合中每个子集合中的一个或两个随机数，从而得到所述个数的随机数。

7.根据权利要求 6 所述的装置，其特征在于，当所述子集合中包括两个随机数时，

所述确定单元，还用于根据所述个数，确定循环周期；

15 根据所述预设阈值，确定分配因子；

根据所述平均数以及所述分配因子，确定最大相差倍数；

根据所述最大相差倍数、所述平均数以及所述循环周期，确定步差；

根据所述步差，确定随机数的偏移范围；

所述确定单元具体用于：

20 确定在所述偏移范围内的第一偏移量；

根据所述最大相差倍数、所述步差、当前步长以及所述第一偏移量，确定所述两个随机数中的第一随机数；

根据所述平均数以及所述第一随机数，确定所述两个随机数中的第二随机数。

8.根据权利要求 6 所述的装置，其特征在于，当所述子集合中包括一个随机数时，

25 所述确定单元，还用于对所述平均数进行随机衰减；

根据随机衰减后的平均数以及预设的最小随机数，确定所述子集合中的一个随机数。

9.根据权利要求 7-8 任一项所述的装置，其特征在于，所述装置还包括：

所述确定单元，还用于根据所述总和以及所述个数的随机数，确定剩余数；

30 拆分单元，用于对所述确定单元确定的所述剩余数进行拆分；

叠加单元，用于将所述拆分单元拆分后的剩余数叠加至所述个数的随机数中，得到更新后的所述个数的随机数。

10.根据权利要求 7-9 任一项所述的装置，其特征在于，所述装置还包括：

排序单元，用于对所述个数的随机数进行重排序；

5 存储单元，用于将所述排序单元重排序后的所述个数的随机数存储到列表中。

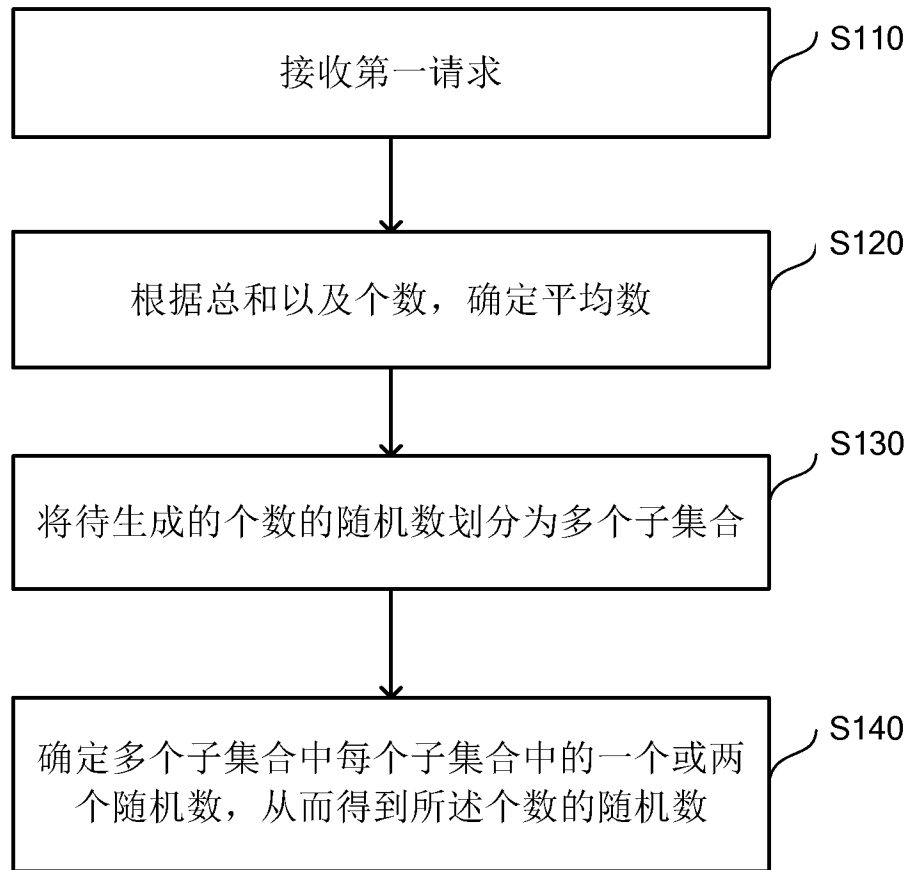


图 1

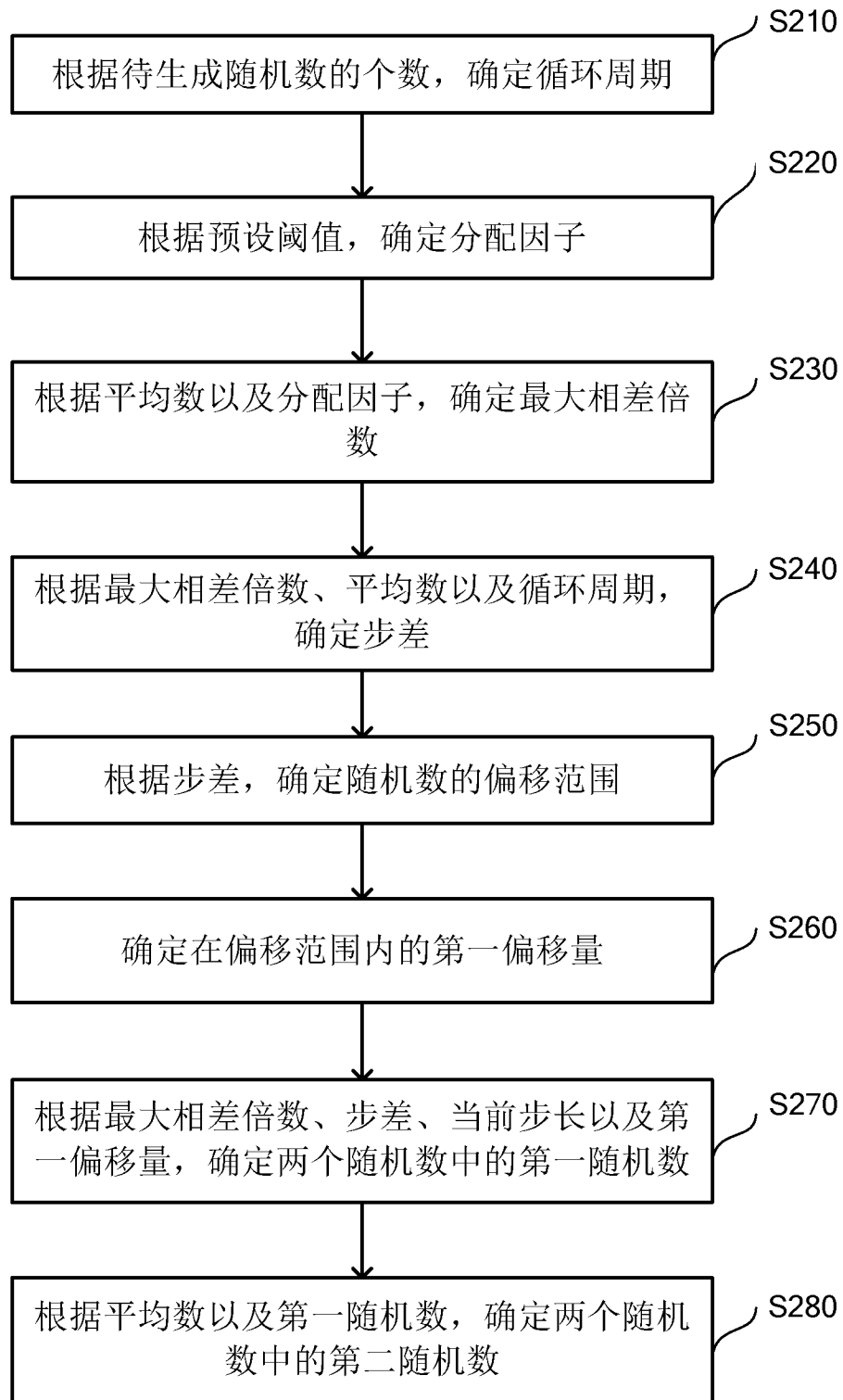


图 2

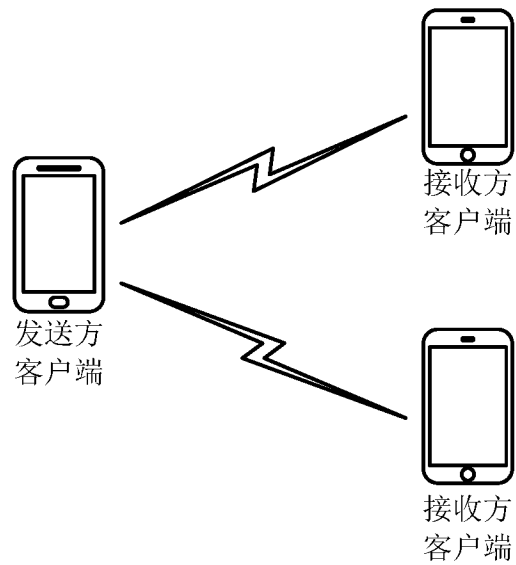


图 3

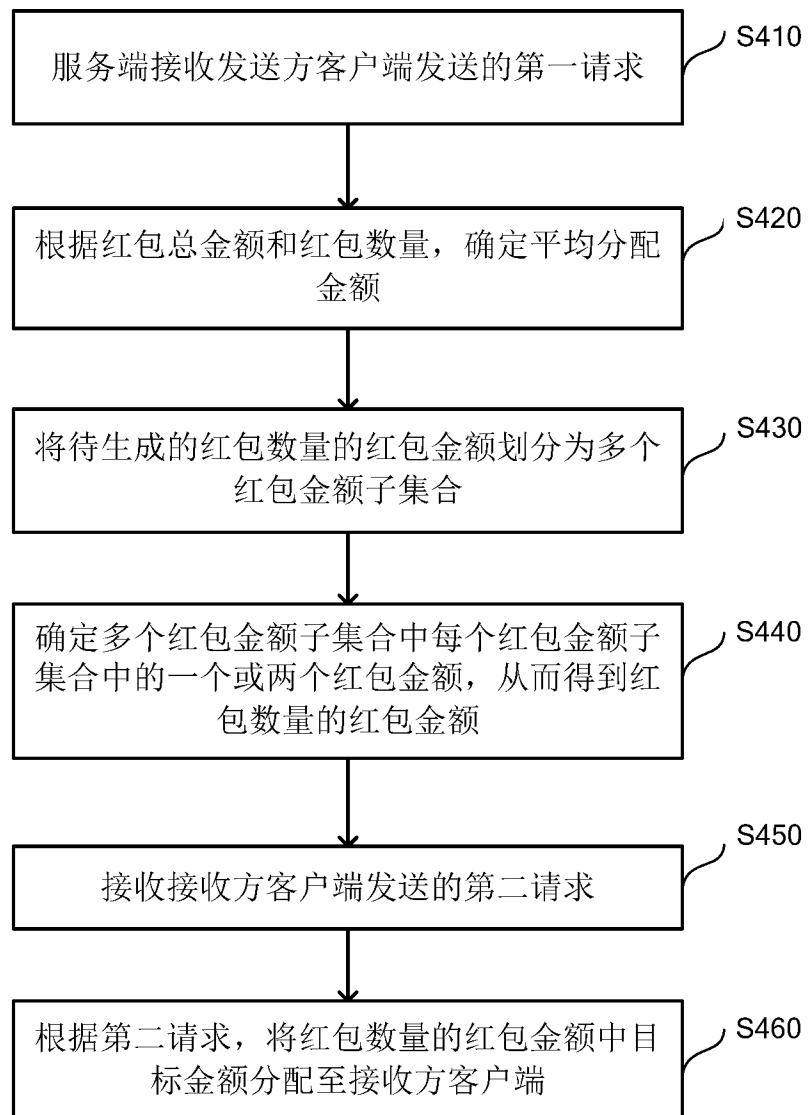


图 4

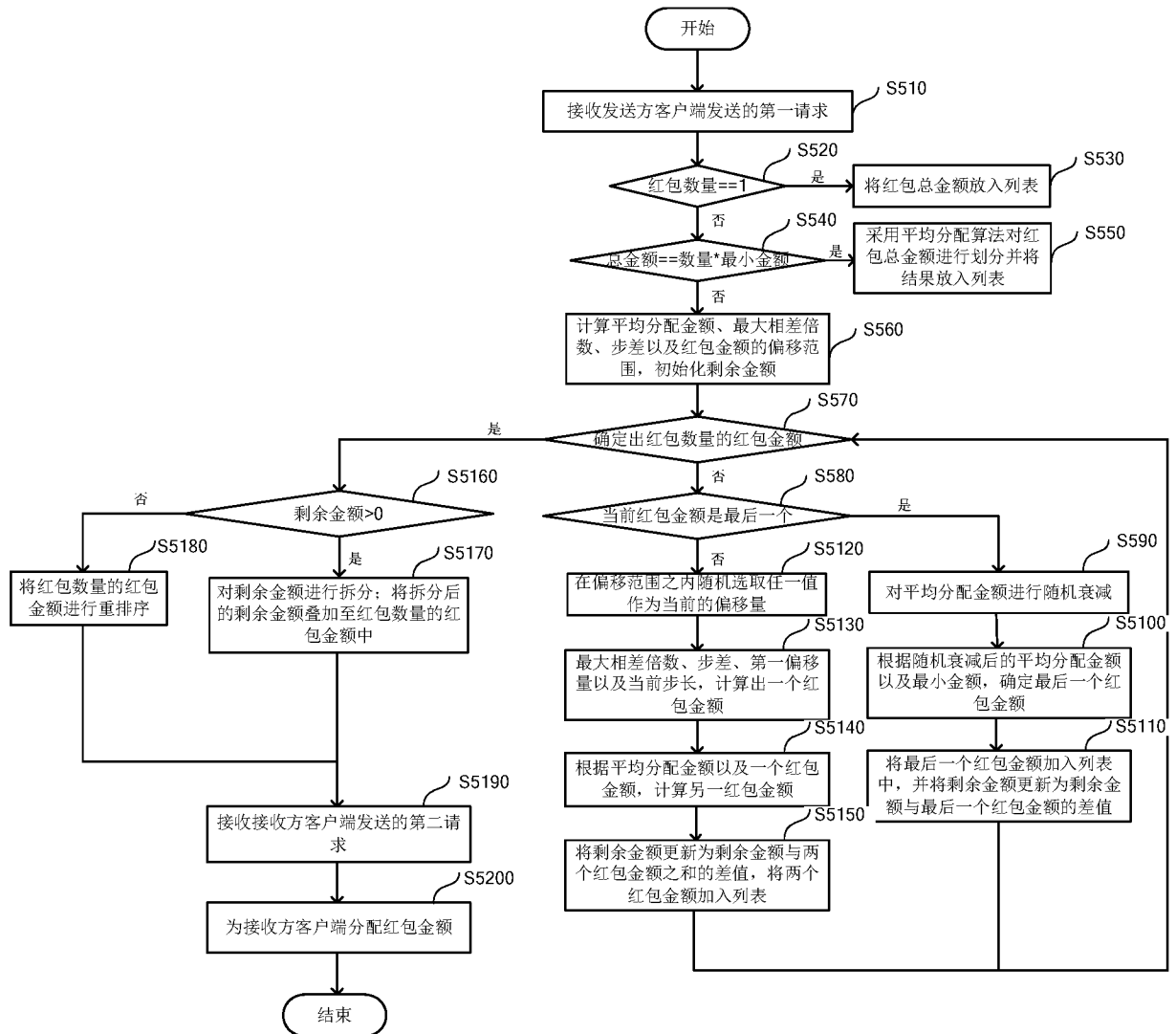


图 5

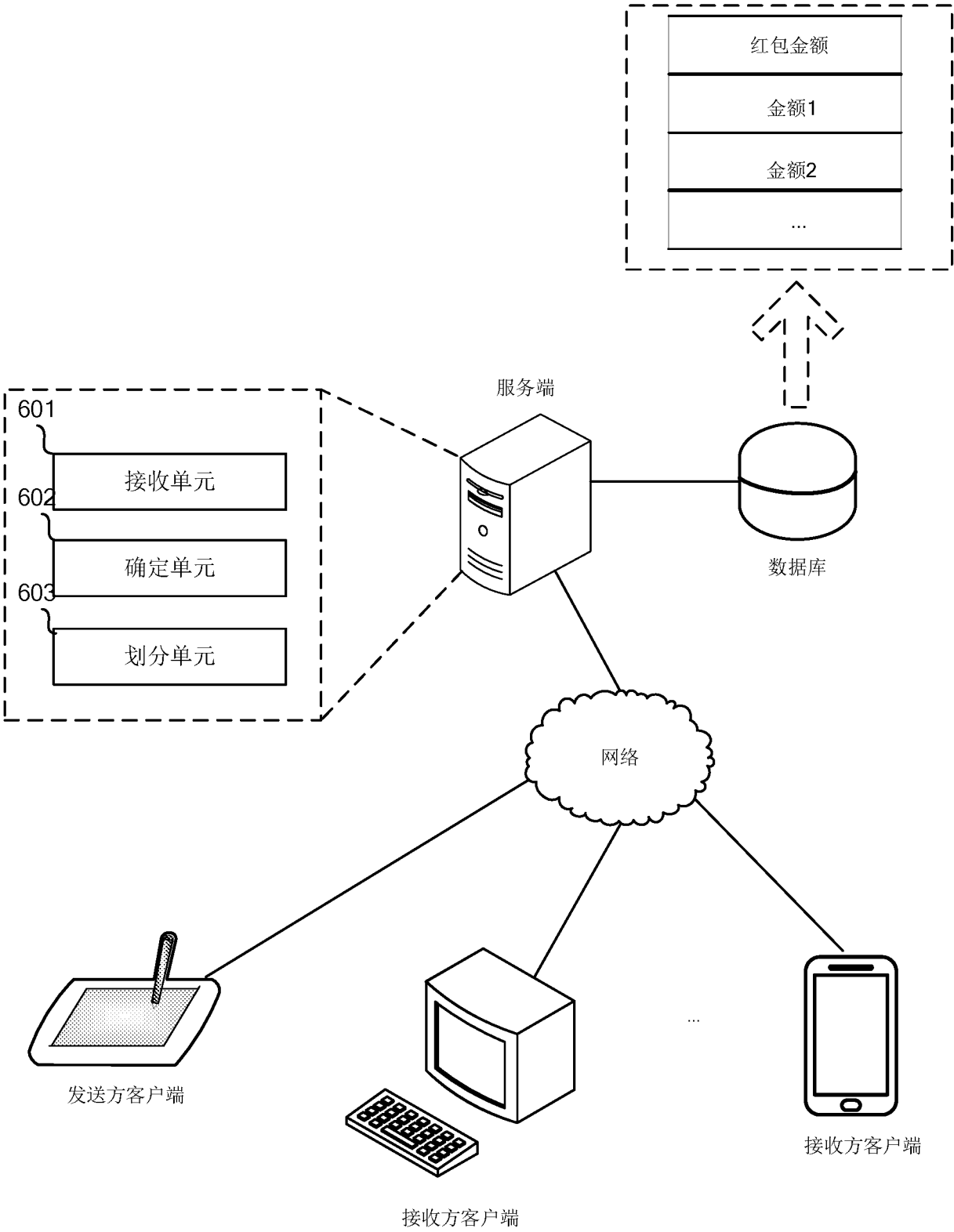


图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/097779

A. CLASSIFICATION OF SUBJECT MATTER

G06F 7/58 (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)

G06F

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)

CNPAT, EPODOC, WPI, CNKI, IEEE: 随机, 数, 生成, 产生, 计算, 总数, 个数, 划分, 分布, 平均, 均匀, 优化, 和, 商, 阈值, 循环, 偏移, 红包, random, number, creat, generation, account, total, partition, distribution, average, equality, optimize, sum, quotient, threshold, cycle, excursion, red-envelop

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 106919365 A (ALIBABA GROUP HOLDING LTD.) 04 July 2017 (04.07.2017), claims 1-10	1-10
A	CN 102799413 A (TSINGHUA UNIVERSITY) 28 November 2012 (28.11.2012), description, paragraphs [0006]-[0027]	1-10
A	CN 101127575 A (ZTE CORPORATION) 20 February 2008 (20.02.2008), entire document	1-10
A	CN 102520908 A (DATANG MICROELECTRONICS TECHNOLOGY CO., LTD.) 27 June 2012 (27.06.2012), entire document	1-10
A	US 2006123073 A1 (SCIENCE APPLICATIONS INTERNATIONAL CORPORATION) 08 June 2006 (08.06.2006), entire document	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 19 October 2017	Date of mailing of the international search report 17 November 2017
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 WU, Yuanyuan Telephone No. (86-10) 52871143

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/097779

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 106919365 A	04 July 2017	None	
CN 102799413 A	28 November 2012	None	
CN 101127575 A	20 February 2008	None	
CN 102520908 A	27 June 2012	None	
US 2006123073 A1	08 June 2006	US 2004153486 A1	05 August 2004
		US 2003005005 A1	02 January 2003

国际检索报告

国际申请号

PCT/CN2017/097779

A. 主题的分类

G06F 7/58(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)

G06F

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))

CNPAT, EPODOC, WPI, CNKI, IEEE: 随机, 数, 生成, 产生, 计算, 总数, 个数, 划分, 分布, 平均, 均匀, 优化, 和, 商, 阈值, 循环, 偏移, 红包, random, number, creat, generation, account, total, partition, distribution, average, equality, optimize, sum, quotient, threshold, cycle, excursion, red-envelop

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
PX	CN 106919365 A (阿里巴巴集团控股有限公司) 2017年 7月 4日 (2017 - 07 - 04) 权利要求1-10	1-10
A	CN 102799413 A (清华大学) 2012年 11月 28日 (2012 - 11 - 28) 说明书第[0006]-[0027]段	1-10
A	CN 101127575 A (中兴通讯股份有限公司) 2008年 2月 20日 (2008 - 02 - 20) 全文	1-10
A	CN 102520908 A (大唐微电子有限公司) 2012年 6月 27日 (2012 - 06 - 27) 全文	1-10
A	US 2006123073 A1 (SCIENCE APPLICATIONS INTERNATIONAL CORPORATION) 2006年 6月 8日 (2006 - 06 - 08) 全文	1-10

☐ 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

2017年 10月 19日

国际检索报告邮寄日期

2017年 11月 17日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
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

吴媛媛

电话号码 (86-10)010-52871143

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/097779

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	106919365	A	2017年 7月 4日	无			
CN	102799413	A	2012年 11月 28日	无			
CN	101127575	A	2008年 2月 20日	无			
CN	102520908	A	2012年 6月 27日	无			
US	2006123073	A1	2006年 6月 8日	US	2004153486	A1	2004年 8月 5日
				US	2003005005	A1	2003年 1月 2日

表 PCT/ISA/210 (同族专利附件) (2009年7月)