

(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 2 月 8 日 (08.02.2018)



(10) 国际公布号
WO 2018/024241 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) **H04W 12/02** (2009.01)
H04W 12/10 (2009.01)

(21) 国际申请号: PCT/CN2017/095990

(22) 国际申请日: 2017 年 8 月 4 日 (04.08.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610640012.X 2016 年 8 月 5 日 (05.08.2016) CN
201610639419.0 2016 年 8 月 5 日 (05.08.2016) CN

(72) 发明人: 及

(71) 申请人: 李明(LI, Ming) [CN/CN]; 中国北京市海淀区太月园12号楼603室, Beijing 100086 (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, 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)。

(54) Title: DATA COMMUNICATION METHOD AND SYSTEM

(54) 发明名称: 一种数据通信方法及系统

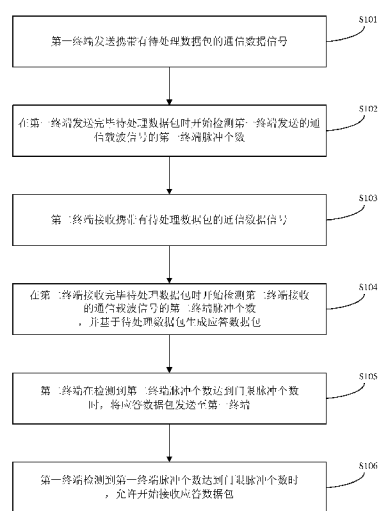


图 1

(57) Abstract: Provided in the present invention are a data communication method and system; when a first terminal finishes sending data packets to be processed, starting to record the number of first terminal pulses of the communication carrier signal sent by the first terminal, and only receiving response data packets when the number of first terminal pulses reaches a threshold number of pulses N; when a second terminal finishes receiving same, starting to record the number of second terminal pulses of the communication carrier signal received by the second terminal, and only sending response data packets when the number of second terminal pulses reaches N; the first terminal and the second terminal implement simultaneous sending and receiving of data on the basis of detecting the number of pulses, greatly increasing the timing accuracy of both sides and thereby ensuring that the first terminal and the second terminal only send and receive response data packets at a specified high accuracy time, preventing the risk of external tampering to the data packets received by the first terminal during the transmission process and increasing the reliability of the response data packets received by the first terminal.

(57) 摘要: 本发明提供一种数据通信方法及系统, 第一终端发送完毕待处理数据包时开始记录第一终端发送的通信载波信号的第一终端脉冲个数, 并仅在第一终端脉冲个数达到门限脉冲个数N时接收应答数据包; 第二终端接收完毕开始记录第二终端接收到的通信载波信号的第二终端脉冲个数, 并仅在第二终端脉冲个数达到N时发送应答数据包, 第一终端与第二终端通过检测脉冲个数进行同时收发数据, 大大提升了双方计时的精确度, 从而保证了第一终端和第二终端仅在特定的高精度时刻收发应答数据包, 避免了第一终端接收到的数据在传输过程中被外界篡改的风险, 提升了第一终端接收到的应答数据包的可靠性。

S101 A first terminal sends a communication data signal carrying data packets to be processed
S102 When the first terminal finishes sending the data packets to be processed, start to detect the number of first terminal pulses of the communication carrier signal sent by the first terminal
S103 A second terminal receives the communication data signal carrying the data packets to be processed
S104 When the second terminal finishes receiving the data packets to be processed, start to detect the number of second terminal pulses of the communication carrier signal received by the second terminal, and on the basis of the data packets to be processed generate response data packets
S105 When detecting that the number of second terminal pulses reaches a threshold number of pulses, the second terminal sends the response data packets to the first terminal
S106 When detecting that the number of first terminal pulses reaches the threshold number of pulses, the first terminal allows the receipt of the response data packets

本国际公布：

- 包括国际检索报告(条约第21条(3))。

一种数据通信方法及系统

相关申请的交叉引用

5 本申请要求李明于 2016 年 8 月 5 日提交中国专利局、申请号为 201610640012.X、发明名称为“一种数据通信方法及系统”的中国专利申请的优先权，以及李明于 2016 年 8 月 5 日提交中国专利局、申请号为 201610639419.0、发明名称为“一种数据通信方法及系统”的中国专利申请的优先权。

技术领域

10 本发明涉及一种电子技术领域，尤其涉及一种数据通信方法及系统。

背景技术

15 现有的非接触式 IC 卡读卡器读卡机制，是基于 14443，15693 等通信协议进行数据传输的，上述协议中，读卡器发送指令数据之后会有一个帧等待时间(Frame Waiting Time, FWT)，表明了读卡器等待接收卡片响应数据的最大时间范围。也就是说在读卡器向卡片发送了指令以后，读卡器就在等待接收卡片的响应数据，只要是在帧等待时间 FWT 之内返回的数据，读卡器就认为返回的数据合法。那么在上述通信协议中，如果中间人截获读卡器发送的数据并在 FWT 时间内返回响应数据，读卡器就会认为数据的来源是可靠的，可见该方案存在被
20 中间人攻击，数据被篡改等安全风险。

发明内容

 本发明旨在解决上述问题之一。

 本发明的主要目的在于提供一种数据通信方法；

25 本发明的另一目的在于提供一种数据通信系统；

 本发明的另一目的在于提供另一种数据通信方法；

 本发明的另一目的在于提供另一种数据通信系统。

 为达到上述目的，本发明的技术方案具体是这样实现的：

30 本发明一方面提供了一种数据通信方法，包括：在第一终端与第二终端通信过程中，所述第一终端始终产生通信载波信号，所述第二终端接收所述通信载波信号，所述方法包括以下步骤：所述第一终端发送携带有待处理数据包的通信数据信号，在所述第一终端发送完毕

所述待处理数据包时开始记录所述第一终端发送的所述通信载波信号的第一终端脉冲个数；所述通信数据信号由所述第一终端将所述待处理数据包调制在所述通信载波信号上得到；所述第二终端接收携带有所述待处理数据包的所述通信数据信号，在所述第二终端接收完毕所述待处理数据包时开始记录所述第二终端接收到的所述通信载波信号的第二终端脉冲个数，并基于所述待处理数据包生成应答数据包；所述第二终端在记录所述第二终端脉冲个数达到门限脉冲个数 N 时，将所述应答数据包发送至所述第一终端；所述第一终端记录所述第一终端脉冲个数达到所述门限脉冲个数 N 时，允许开始接收所述应答数据包。

本发明一方面还提供了一种数据通信系统，至少包括第一终端，第二终端，在所述第一终端与所述第二终端通信过程中，所述第一终端始终产生通信载波信号，所述第一终端，用于发送携带有待处理数据包的通信数据信号，在所述第一终端发送完毕所述待处理数据包时开始记录所述第一终端发送的所述通信载波信号的第一终端脉冲个数；所述通信数据信号由所述第一终端将所述待处理数据包调制在所述通信载波信号上得到；所述第二终端，用于接收携带有所述待处理数据包的所述通信数据信号，在所述第二终端接收完毕所述待处理数据包时开始记录所述第二终端接收到的所述通信载波信号的第二终端脉冲个数，并基于所述待处理数据包生成应答数据包；所述第二终端，用于在记录所述第二终端脉冲个数达到门限脉冲个数 N 时，将所述应答数据包发送至所述第一终端；所述第一终端，用于在记录所述第一终端脉冲个数达到所述门限脉冲个数 N 时，允许开始接收所述应答数据包。

由上述本发明提供的技术方案可以看出，本发明提供了一种数据通信方法与一种数据通信系统，第一终端发送完毕待处理数据包时开始记录第一终端发送的通信载波信号的第一终端脉冲个数，并仅在第一终端脉冲个数达到门限脉冲个数 N 时接收应答数据包；第二终端接收完毕开始记录第二终端接收到的通信载波信号的第二终端脉冲个数，并仅在第二终端脉冲个数达到 N 时发送应答数据包，第一终端与第二终端通过检测脉冲个数进行同时收发数据，大大提升了双方计时的精确度，从而保证了第一终端和第二终端仅在特定的高精度时刻收发应答数据包，即使第二终端向第一终端发送的应答数据包在传输过程中被第三方截获，由于第三方对数据的篡改时间为毫秒级别，远远大于第一终端的计时精度，第一终端在特定时刻未接收到应答数据包立即停止通信流程，第三方篡改后的数据到达第一终端时，第一终端已终止通信流程，从而杜绝了第一终端接收到的数据在传输过程中被外界篡改的风险，大大提升了第一终端接收到的应答数据包的可靠性。

本发明另一方面还提供了另一种数据通信方法，在第一终端与第二终端通信过程中，第一终端始终产生通信载波信号，第二终端接收通信载波信号，方法包括以下步骤：第一终端

发送携带有待处理数据包的通信数据信号，在第一终端发送完毕待处理数据包时开始记录第一终端发送的通信载波信号的第一终端脉冲个数；通信数据信号由第一终端将待处理数据包调制在通信载波信号上得到；第二终端接收携带有待处理数据包的通信数据信号，在第二终端接收完毕待处理数据包时开始记录第二终端接收到的通信载波信号的第二终端脉冲个数，并基于待处理数据包生成应答数据包；第二终端在检测到第二终端脉冲个数达到门限脉冲个数 N 时，将应答数据包发送至第一终端；第一终端在检测到第一终端脉冲个数在门限范围内时，允许开始接收应答数据包，其中，门限范围为第一终端基于门限脉冲个数 N 获得。

本发明的另一方面还提供了另一种数据通信系统，至少包括第一终端，第二终端，在第一终端与第二终端通信过程中，第一终端始终产生通信载波信号，第二终端接收通信载波信号，第一终端，用于发送携带有待处理数据包的通信数据信号，在第一终端发送完毕待处理数据包时开始记录第一终端发送的通信载波信号的第一终端脉冲个数；通信数据信号由第一终端将待处理数据包调制在通信载波信号上得到；第二终端，用于接收携带有待处理数据包的通信数据信号，在第二终端接收完毕待处理数据包时开始记录第二终端接收到的通信载波信号的第二终端脉冲个数，并基于待处理数据包生成应答数据包；第二终端在检测到第二终端脉冲个数达到门限脉冲个数 N 时，将应答数据包发送至第一终端；第一终端在检测到第一终端脉冲个数在门限范围内时，允许开始接收应答数据包，其中，门限范围为第一终端基于门限脉冲个数 N 获得。

由上述本发明提供的技术方案可以看出，本发明提供了一种数据通信方法与一种数据通信系统，第一终端发送完毕待处理数据包时开始记录第一终端发送的通信载波信号的第一终端脉冲个数，并仅在第一终端脉冲个数符合门限范围时接收应答数据包；第二终端接收完毕开始记录第二终端接收到的通信载波信号的第二终端脉冲个数，并仅在第二终端脉冲个数达到 N 时发送应答数据包，第一终端与第二终端通过检测脉冲个数进行同时收发数据，大大提升了双方计时的精确度，从而保证了第一终端和第二终端仅在特定的高精度时刻收发应答数据包，即使第二终端向第一终端发送的应答数据包在传输过程中被第三方截获，由于第三方对数据的篡改时间为毫秒级别，远远大于第一终端的计时精度，第一终端在特定时刻未接收到应答数据包立即停止通信流程，第三方篡改后的数据到达第一终端时，第一终端已终止通信流程，从而杜绝了第一终端接收到的数据在传输过程中被外界篡改的风险，大大提升了第一终端接收到的应答数据包的可靠性

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，对于本领域的

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他附图。

图 1 为本发明实施例 1 提供了一种数据通信方法的流程图；

图 2 为本发明实施例 1 提供的门限脉冲个数协商方法流程图；

图 3 为本发明实施例 1 提供了一种数据通信系统的结构框图；

5 图 4 为本发明实施例 2 提供了一种数据通信方法的流程图。

具体实施方式

下面结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明的实
10 施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明的保护范围。

下面将结合附图对本发明实施例作进一步地详细描述。

实施例 1

15 本实施例提供一种数据通信方法，在第一终端与第二终端通信过程中，第一终端始终产生通信载波信号，在通信技术上，通信载波信号是由振荡器产生并在通讯信道上传输的电波，被调制后用来传送数据，在本实施例中，通信载波由第一终端产生，作为传送数据信息的承载工具。

如附图 1 所示，包括以下步骤：

20 S101，第一终端发送携带有待处理数据包的通信数据信号，

通信数据信号由第一终端将待处理数据包调制在通信载波信号上得到，通信载波信号为未受调制的周期性振荡信号，通信载波信号可以是正弦波，也可以是非正弦波（如周期性脉冲序列），将待处理数据包调制到通信载波信号后产生的信号称为通信数据信号，它含有待处理数据包的全波特征。一般要求通信载波信号的频率远远高于待处理数据包调制信号的带
25 宽，否则会发生混叠，使传输信号失真。使用通信数据信号传输，第一终端将待处理数据包的信号加载到通信载波信号上进行数据传输，保证待处理数据包的正确外发。

S102，在第一终端发送完毕待处理数据包时开始记录第一终端发送的通信载波信号的第一终端脉冲个数；通信数据信号由第一终端将待处理数据包调制在通信载波信号上得到；

在通信领域中，脉冲信号是一种离散信号，可以拥有多种形式，例如尖脉冲信号、三角
30 波脉冲信号等，与普通模拟信号相比，脉冲信号的波形之间在时间轴不连续，波形与波形之间有明显的间隔，但具有一定的周期性。最常见的脉冲信号是矩形波，也就是方波，表现形式为周期性的高电平或周期性的低电平。在本实施例中，第一终端与第二终端通过记录脉冲

信号的脉冲个数进行计时收发信号。第一终端发送完毕待处理数据包时，从个数 0 开始实时记录通信载波信号的脉冲个数，从而实时获得第一终端发送的通信载波信号的第一终端脉冲个数；或者，第一终端发送完毕待处理数据包时，利用第一终端内部的脉冲检测元件检测当前的脉冲个数，并将当前的脉冲个数设置为第一起始脉冲个数，之后开始实时检测通信载波信号的脉冲个数变化，从而实时获得通信载波信号的脉冲相对于第一起始脉冲个数的差值。通信载波信号的脉冲个数变化速度与通信载波信号的频率正相关，通过检测某一 T 时刻第一终端发送的通信载波信号的第一终端脉冲个数，能够基于脉冲个数精确记录 T 时刻与第一终端发送完毕待处理数据包时刻之间的时间间隔，例如，当通信载波信号的频率为 ν 时，其一个周期的持续时间为 $\frac{1}{\nu}$ ，也就是说其相邻两个脉冲的间隔时间为 $\frac{1}{\nu}$ ，由于通信载波信号的频率一般都为极高值，例如 13.56MHz、2.4GHz，当通信载波信号采用的频率为 2.4GHz 时，其相邻两个脉冲的间隔时间约为 0.4 纳秒，可见，第一终端通过测量通信载波信号脉冲个数变化来检测时间间隔能够大大提升检测精度。

S103，第二终端接收携带有待处理数据包的通信数据信号，

第二终端按照通信载波信号的频率来接收待处理数据包数据信号，有意义的信号波的波幅与无意义的信号的波幅是不同，将有效信号提取出来就是需要的待处理数据包的数据信号，从而高效获得待处理数据包。

S104，在第二终端接收完毕待处理数据包时开始记录第二终端接收到的通信载波信号的第二终端脉冲个数，并基于待处理数据包生成应答数据包；

第二终端接收完毕待处理数据包时，从个数 0 开始实时记录通信载波信号的脉冲个数，从而实时获得第二终端接收的通信载波信号的第二终端脉冲个数；或者，第二终端接收完毕待处理数据包时，利用第二终端内部的脉冲检测元件检测当前的脉冲个数，并将当前的脉冲个数设置为第二起始脉冲个数，之后开始实时检测通信载波信号的脉冲个数变化，从而实时获得通信载波信号的脉冲相对于第二起始脉冲个数的差值，并对接收到的待处理数据包进行处理操作，生成应答数据包；第二终端通过检测第一终端发送的通信载波信号进行计时，无需在第二终端设置计时器、晶振、电源等元件就能够实现时间间隔的测量，降低了第二终端的生产成本；通过检测某一 T 时刻第二终端接收的通信载波信号的第一终端脉冲个数，能够基于脉冲个数精确记录 T 时刻与第二终端接收完毕待处理数据包时刻之间的时间间隔，例如，当通信载波信号的频率为 ν 时，其一个周期的持续时间为 $\frac{1}{\nu}$ ，也就是说其相邻两个脉冲的间隔时间为 $\frac{1}{\nu}$ ，由于通信载波信号的频率一般都为极高值，例如 13.56MHz、2.4GHz，当通信载波信号采用的频率为 2.4GHz 时，其相邻两个脉冲的间隔时间约为 0.4 纳秒，可见，第二终端通过通过测量通信载波信号脉冲个数变化来检测时间间隔能够大大提升检测精度；

第一终端与第二终端基于同一通信载波信号的脉冲个数变化进行时间检测,当第一终端发送完毕待处理数据包后,在 $T1$ 时刻开始检测通信载波信号的脉冲个数变化,当第二终端接收完毕待处理数据包后,在 $T2$ 时刻开始检测通信载波信号的脉冲个数变化, $T2=T1+\Delta T1+\Delta T2$,第一终端将待处理数据包拆分为 x 个数据块进行发送,其中, $\Delta T1$ 为待处理数据包中的第 x 个数据块在第一终端与第二终端之间的传输时间, $\Delta T2$ 为第 x 个数据块到达第二终端的时刻与第二终端接收完毕待处理数据包第 x 个数据块的时刻之间的时间差;待处理数据包在传输过程中为光速传输,待处理数据包最后一个数据块的传输时间 $\Delta T1$ 为传输距离 S 与光速 C 的比值,即 $\Delta T1=S/C$,由于 $C=3\times 10^8\text{ m/s}$,因此 $\Delta T1$ 为一个极小值;通常情况下,通信双方在数据包的交互过程中,会将待传输的数据包拆分为多个数据块进行发送,在本实施例例中,假设将待传输的数据包拆分为 x 个数据块进行发送,第一终端在发送完毕最后一个数据块即第 x 个数据块之前,第二终端已开始接收到待处理数据包中的第一个数据块,在 $T1+\Delta T1$ 时刻时,第二终端已接收完毕待处理数据包中 $x-1$ 个数据块, $\Delta T2$ 为第 x 个数据块到达第二终端的时刻与第二终端接收完毕待处理数据包第 x 个数据块的时刻之间的时间差,因此 $\Delta T2$ 也为一个极小值,因此,在本实施例提供的通信方法中,第一终端与第二终端可以等效看作同时基于通信载波信号进行计时,这就保证了双方计时结果的同步性与精确性;

第二终端接收到待处理数据包后,对待处理数据包进行认证操作,认证成功后提取待处理数据包中的关键信息,对关键信息进行处理,生成应答数据包,例如在交易通信中,第二终端接收到待处理数据包后,对待处理数据包进行验签操作,确认第一终端的身份合法,之后提取待处理数据包中的交易账号、交易金额等关键信息并显示,用户进行确认后第二终端利用第二终端私钥对关键信息进行签名操作,生成签名数据,并基于签名数据与第二终端证书生成应答数据包,从而保证通信的安全性。

S105,第二终端在记录第二终端脉冲个数达到门限脉冲个数 N 时,将应答数据包发送至第一终端;

第二终端实时检测当前时刻通信载波信号脉冲个数相对于第二起始脉冲个数的变化差值,当变化差值达到门限脉冲个数 N 时,将生成的应答数据包发送至第一终端,门限脉冲个数 N 可以为第一终端和第二终端存储于出厂设置信息中,或者,门限脉冲个数 N 可以为第一终端和第二终端协商生成,或者,门限脉冲个数 N 可以携带在第一终端和第二终端的通信协议中,其中,可选地, $\omega \leq N \leq \lambda$, ω 为通信载波信号经过第二终端对接收到的第一终端发送的数据进行处理的预定完成时间所产生的脉冲个数变化值,预定完成时间是指第二终端处理完成第一终端发送的数据所需要的最长时间, $N \geq \omega$ 能够保证第二终端在需要发送应答数据包之前,完成对待处理数据包的处理操作并生成应答数据包,保证第一终端与第二

终端之间的正常通信得以实现； λ 为通信载波信号经过第一终端与第二终端采用的通信协议规定的帧等待时间所产生的脉冲个数变化值，帧等待时间是指通信协议中规定的待处理数据包发出后的有效等待时间，超出帧等待时间后判断通信失败，第一终端与第二终端采用的通信协议可以为目前通用的通信协议以及未来可能会出现的通信协议，例如 ISO14443 通信协议、ISO15693 通信协议， $N \leq \lambda$ 能够保证第二终端在帧等待时间内将应答数据包发送至第一终端，兼容现有的通信协议，保证在现有通信协议下第一终端与第二终端之间能够进行正常通信；第二终端通过检测脉冲个数并在第二脉冲个数达到门限脉冲个数 N 时外发应答数据包，使应答数据包仅在特定的时间点外发，同时保证了应答数据包发送时刻的精确度。

S106，第一终端记录第一终端脉冲个数达到门限脉冲个数 N 时，允许开始接收应答数据包；

在本实施例中，第一终端和第二终端采用短距离无线通信方式进行通信，短距离无线通信方式可以包括以下通信协议：蓝牙通信协议、红外 IrDA 通信协议、RFID 通信协议、ZigBee 通信协议、超宽频(Ultra WideBand) 通信协议、短距通信(NFC) 通信协议、WiMedia 通信协议、GPS 通信协议、DECT 通信协议、无线 1394 通信协议和专用无线通信协议，采用上述短距离无线通信方式进行通信时，第一终端与第二终端之间的距离相对于数据信号在单位时间内的传送距离可以忽略不计，例如采用蓝牙通信协议进行通信时第一终端与第二终端之间的距离小于 10 米，第一终端与第二终端之间的数据以光速进行无线传输，那么在这种短距离无线通信方式下，第一终端与第二终端之间的数据传输时间极短，约为 30ns，可以忽略不计，也就是说，在第一终端发送数据包后，第二终端立即能够接收到数据包，第一终端接收到第二终端在检测到第二终端脉冲个数达到门限脉冲个数 N 时外发的应答数据包时，第一终端检测到的第一终端脉冲个数同样为 N ；第一终端仅在检测到第一终端脉冲个数达到门限脉冲个数 N 时，允许开始接收所述应答数据包，否则，第一终端不允许接收外部发送的数据信息，这就大大提升了接收到的应答数据包的可靠性。本实施例中，第一终端与第二终端可以为能够进行数据交互通信的任意设备，可选地，第一终端可以为读取器，该读取器可以为读卡器、计算机、手机、路由器、车载设备、服务器等设备，第二终端可以为应答器，该应答器可以为智能卡、身份证、智能密钥设备、手机、计算机、路由器、智能家居、可穿戴设备等设备，在数据通信过程中，第一终端与第二终端通过检测脉冲个数进行同时收发大大提升了双方计时的精确度，从而保证了第一终端和第二终端仅在特定的高精度时刻收发应答数据包，即使第二终端向第一终端发送的应答数据包在传输过程中被第三方截获，由于第三方对数据的篡改时间为毫秒级别，远远大于第一终端的计时精度，第一终端在特定时刻未接收到应答数据包立即停止通信流程，第三方篡改后的数据到达第一终端时，第一终端已终止通信流程，从而杜绝了第一终端接收到的数据在传输过程中被外界篡改的风险，大大提升了

第一终端接收到的应答数据包的可靠性。

可选地，在步骤 S101 第一终端发送携带有待处理数据包的通信数据信号之前，如图 2 所示，还包括步骤：

S1001，第一终端生成通信请求，并将通信请求发送至第二终端；

5 S1002，第二终端接收通信请求，基于通信请求生成第一协商数据包，并将第一协商数据包发送至第一终端；

S1003，第一终端接收第一协商数据，基于第一协商数据对第二终端进行认证操作，认证成功，生成第二协商数据包，并将第二协商数据包发送至第二终端；

10 S1004，第二终端接收第二协商数据包，基于第二协商数据包对第一终端进行认证操作，认证成功后，生成门限脉冲个数 N ，对门限脉冲个数 N 进行加密操作，生成门限脉冲个数密文，并将门限脉冲个数密文发送至第一终端，其中， $N \leq \lambda$ ， λ 为通信载波信号经过第一终端与第二终端采用的通信协议规定的帧等待时间所产生的脉冲个数；

帧等待时间是指通信协议中规定的待处理数据包发出后的有效等待时间，超出帧等待时间后判断通信失败， $N \leq \lambda$ 能够保证第二终端在帧等待时间内将应答数据包发送至第一终端，兼容现有的通信协议，保证在现有通信协议下第一终端与第二终端之间能够进行正常通信；

15 可选地， $\omega \leq N \leq \lambda$ ，其中， ω 为通信载波信号经过第二终端对接收到的第一终端发送的数据进行处理的预定完成时间所产生的脉冲个数变化值，第一终端可以采用多种方式获取，包括但不限于以下方式： ω 可以为第一终端通过外部按键输入获得、 ω 可以为第二终端发送至第一终端获得、 ω 可以为第一终端扫码获得、 ω 可以为第一终端根据出厂预设信息获得； $N \geq \omega$ 能够保证第二终端在需要发送应答数据包之前，完成对待处理数据包的处理操作并生成应答数据包，保证第一终端与第二终端之间的正常通信得以实现；

S1005，第一终端接收门限脉冲个数密文，对门限脉冲个数密文进行解密操作，获得门限脉冲个数 N 并存储。

步骤 S1001 至 S1005 可以包括但不限于本实施例提供的以下 3 种实现方案：

25 方案 1：

第一终端生成第一随机数，并将第一随机数发送至第二终端；

第一随机数可以是第一终端根据外部的随机噪声信号生成，也可以是根据内部的随机数生成器生成，保证第一随机数的外部不可获取性；

30 第二终端接收第一随机数，生成第二随机数，利用第二设备私钥对第一随机数进行签名操作，生成第一签名信息，并将第一协商数据包发送至第一终端，其中，第一协商数据包至少包括：第二终端的 CA 证书、第一签名信息、第二随机数；

第二随机数可以是第二终端根据外部的随机噪声信号生成，也可以是根据内部的随机数

生成器生成，保证第二随机数的外部不可获取性；第二设备基于自身私钥对第一随机数进行签名操作，并将自身 CA 证书发送至第一终端，以使第一终端对自身的合法性进行认证；

第一终端接收第一协商数据，对第二终端的 CA 证书进行认证操作，认证成功后，获得第二终端公钥，基于第二终端公钥对第一签名信息进行验签操作，验签成功后，利用第一设备私钥对第二随机数进行签名操作，生成第二签名信息，并将第二协商数据包发送至第二终端，其中，第二协商数据包至少包括：第一终端的 CA 证书、第二签名信息；

第一终端基于第二终端公钥对第二终端进行身份认证，保证第二终端的合法性，认证成功后，第一设备基于自身私钥对第二随机数进行签名操作，并将自身 CA 证书发送至第二终端，以使第二终端对自身的合法性进行认证；

第二终端接收第二协商数据，对第一终端的 CA 证书进行认证操作，认证成功后，获得第一终端公钥，基于第一终端公钥对第二签名信息进行验签操作，验签成功后，生成门限脉冲个数 N ，利用第一终端公钥对门限脉冲个数 N 进行加密操作，生成门限脉冲个数密文，并将门限脉冲个数密文发送至第一终端；

第二终端基于第一终端公钥对第一终端进行身份认证，保证第一终端的合法性，认证成功后，生成门限脉冲个数 N ，并利用第一终端公钥对门限脉冲个数进行加密操作，生成门限脉冲个数密文，由于利用第一终端公钥对门限脉冲个数进行加密操作生成的门限脉冲个数密文只能用第一终端私钥进行解密，而第一终端私钥保存在第一终端安全芯片内部，外界无法获得，从而保证了门限脉冲个数 N 的安全性；

第一终端接收门限脉冲个数密文，利用第一终端私钥对门限脉冲个数密文进行解密操作，获得门限脉冲个数 N 并存储；

第一终端利用自身私钥对门限脉冲个数密文进行解密，获得门限脉冲个数 N 并存储，实现第一终端与第二终端之间的门限脉冲个数 N 协商，同时保证了协商过程的安全性。

方案 2:

第一终端生成第一随机数，并将第一随机数与第一终端的 CA 证书发送至第二终端；

第一随机数可以是第一终端根据外部的随机噪声信号生成，也可以是根据内部的随机数生成器生成，保证第一随机数的外部不可获取性；

第二终端接收第一随机数与第一终端的 CA 证书，生成第二随机数，对第一终端的 CA 证书进行认证操作，认证成功后，获得第一终端公钥，利用第二终端私钥对第一随机数进行签名操作，生成第一签名信息，利用第一终端公钥对第二随机数进行加密操作，生成第二随机数密文，并将第一协商信息发送至第一终端，其中，第一协商信息至少包括：第二终端的 CA 证书、第一签名信息、第二随机数密文；

第二随机数可以是第二终端根据外部的随机噪声信号生成，也可以是根据内部的随机数

生成器生成, 保证第二随机数的外部不可获取性; 第二终端基于第一终端 CA 证书获得第一终端公钥, 并利用第一终端公钥对第二随机数进行加密, 由于利用第一终端公钥加密生成的第二随机数密文只能用第一终端私钥进行解密, 而第一终端私钥保存在第一终端安全芯片内部, 外界无法获得, 从而保证了第二随机数的安全性;

5 第一终端接收第一协商数据, 对第二终端的 CA 证书进行认证操作, 认证成功后, 基于第二终端公钥对第一签名信息进行验签操作, 验签成功后, 利用第一设备私钥对第二随机数密文进行解密操作, 获得第二随机数, 利用第一设备私钥对第二随机数进行签名操作, 生成第二签名信息; 第一终端生成第三随机数, 利用第二设备公钥对第三随机数进行加密, 获得第三随机数密文, 基于第二随机数与第三随机数根据第一预设算法获得传输密钥, 并将第二协商信息发送至第二终端, 其中, 第二协商信息至少包括: 第二签名信息、第三随机数密文;

10 第一终端基于第二终端公钥对第二终端进行身份认证, 保证第二终端的合法性, 认证成功后, 利用自身私钥对第二随机数密文进行解密, 获得第二随机数, 生成第三随机数, 基于第二随机数与第三随机数根据第一预设算法获得传输密钥; 第三随机数可以是第一终端根据外部的随机噪声信号生成, 也可以是根据内部的随机数生成器生成, 保证第三随机数的外部不可获取性; 利用第二终端公钥对第三随机数进行加密, 由于利用第二终端公钥加密生成的第三随机数密文只能用第二终端私钥进行解密, 而第二终端私钥保存在第二终端安全芯片内部, 外界无法获得, 从而保证了第三随机数的安全性;

15 第二终端接收第二协商数据, 基于第一终端公钥对第二签名信息进行验签操作, 验签成功后, 利用第二终端私钥对第三随机数密文进行解密操作, 获得第三随机数, 基于第二随机数与第三随机数根据第一预设算法获得传输密钥; 第二终端生成传输密钥生成反馈信息, 并将传输密钥生成反馈信息发送至第一终端;

20 第二终端利用自身私钥解密第三随机数密文后, 获得第三随机数, 基于第二随机数与第三随机数根据第一预设算法获得传输密钥, 由于第一终端与第二终端各自基于第二随机数与第三随机数根据第一预设算法获得传输密钥, 既保证了双方协商出同一传输密钥, 又无需将传输密钥外发避免了传输密钥在通信过程中外泄, 提升了通信的安全性;

25 第一终端接收传输密钥生成反馈信息, 生成门限脉冲个数 N , 利用传输密钥对门限脉冲个数 N 进行加密, 生成门限脉冲个数密文, 并将门限脉冲个数密文发送至第二终端;

30 第一终端生成门限脉冲个数 N , 并利用传输密钥对门限脉冲个数进行加密操作, 生成门限脉冲个数密文, 由于传输密钥是第一终端与第二终端各自基于第二随机数与第三随机数根据第一预设算法获得, 仅存于第一终端与第二终端内部, 外界无法获得, 从而保证了门限脉冲个数 N 的安全性;

第二终端接收门限脉冲个数密文, 利用传输密钥对门限脉冲个数密文进行解密, 获得门

限脉冲个数 N 并存储;

第二终端利用传输密钥对门限脉冲个数密文进行解密, 获得门限脉冲个数 N 并存储, 实现第一终端与第二终端之间的门限脉冲个数 N 的协商, 同时保证了协商过程的安全性。

方案 3:

5 第一终端生成第一随机数, 并将第一随机数与第一终端的 CA 证书发送至第二终端;

第一随机数可以是第一终端根据外部的随机噪声信号生成, 也可以是根据内部的随机数生成器生成, 保证第一随机数的外部不可获取性;

10 第二终端接收第一随机数与第一终端的 CA 证书, 生成第二随机数, 对第一终端的 CA 证书进行认证操作, 认证成功后, 获得第一终端公钥, 利用第二终端私钥对第一随机数进行签名操作, 生成第一签名信息, 利用第一终端公钥对第二随机数进行加密操作, 生成第二随机数密文, 并将第一协商信息发送至第一终端, 其中, 第一协商信息至少包括: 第二终端的 CA 证书、第一签名信息、第二随机数密文;

15 第二随机数可以是第二终端根据外部的随机噪声信号生成, 也可以是根据内部的随机数生成器生成, 保证第二随机数的外部不可获取性; 第二终端基于第一终端 CA 证书获得第一终端公钥, 并利用第一终端公钥对第二随机数进行加密, 由于利用第一终端公钥加密生成的第二随机数密文只能用第一终端私钥进行解密, 而第一终端私钥保存在第一终端安全芯片内部, 外界无法获得, 从而保证了第二随机数的安全性;

20 第一终端接收第一协商数据, 对第二终端的 CA 证书进行认证操作, 认证成功后, 基于第二终端公钥对第一签名信息进行验签操作, 验签成功后, 利用第一设备私钥对第二随机数密文进行解密操作, 获得第二随机数, 利用第一设备私钥对第二随机数进行签名操作, 生成第二签名信息; 第一终端生成第三随机数, 利用第二设备公钥对第三随机数进行加密, 获得第三随机数密文, 基于第二随机数与第三随机数根据第一预设算法获得传输密钥, 并将第二协商信息发送至第二终端, 其中, 第二协商信息至少包括: 第二签名信息、第三随机数密文;

25 第一终端基于第二终端公钥对第二终端进行身份认证, 保证第二终端的合法性, 认证成功后, 利用自身私钥对第二随机数密文进行解密, 获得第二随机数, 生成第三随机数, 基于第二随机数与第三随机数根据第一预设算法获得传输密钥; 第三随机数可以是第一终端根据外部的随机噪声信号生成, 也可以是根据内部的随机数生成器生成, 保证第三随机数的外部不可获取性; 利用第二终端公钥对第三随机数进行加密, 由于利用第二终端公钥加密生成的第三随机数密文只能用第二终端私钥进行解密, 而第二终端私钥保存在第二终端安全芯片内部, 外界无法获得, 从而保证了第三随机数的安全性;

30 第二终端接收第二协商数据, 基于第一终端公钥对第二签名信息进行验签操作, 验签成功后, 利用第二终端私钥对第三随机数密文进行解密操作, 获得第三随机数, 基于第二随机

数与第三随机数根据第一预设算法获得传输密钥；第二终端生成门限脉冲个数 N ，利用传输密钥对门限脉冲个数 N 进行加密，生成门限脉冲个数密文，并将门限脉冲个数密文发送至第一终端；

第二终端利用自身私钥解密第三随机数密文后，获得第三随机数，基于第二随机数与第三随机数根据第一预设算法获得传输密钥，由于第一终端与第二终端各自基于第二随机数与第三随机数根据第一预设算法获得传输密钥，既保证了双方协商出同一传输密钥，又无需将传输密钥外发避免了传输密钥在通信过程中外泄，提升了通信的安全性；第二终端生成门限脉冲个数 N ，并利用传输对门限脉冲个数 N 进行加密操作，生成门限脉冲个数密文，由于传输密钥是第一终端与第二终端各自基于第二随机数与第三随机数根据第一预设算法获得，仅存于第一终端与第二终端内部，外界无法获得，从而保证了门限脉冲个数 N 的安全性；

第一终端接收门限脉冲个数密文，利用传输密钥对门限脉冲个数密文进行解密，获得门限脉冲个数 N 并存储；

第一终端利用传输密钥对门限脉冲个数密文进行解密，获得门限脉冲个数 N 并存储，实现第一终端与第二终端之间的门限脉冲个数 N 的协商，同时保证了协商过程的安全性。

通过上述门限脉冲个数 N 的协商过程，能够保证门限脉冲个数 N 生成的安全性，避免门限脉冲个数 N 被外部获取，进一步地，上述门限脉冲个数 N 的协商过程可以在每次信息交互之前重新协商生成，从而进一步保证门限脉冲个数 N 的安全性。

可选地，第一终端与第二终端的出厂预置信息中存储有门限脉冲个数 N ，其中， $N \leq \lambda$ ， λ 为通信载波信号经过第一终端与第二终端采用的通信协议规定的帧等待时间所产生的脉冲个数；

通过在第一终端与第二终端的出厂预置信息中存储有门限脉冲个数 N ，能够实现无需在第一终端与第二终端之间传输门限脉冲个数 N ，从而避免门限脉冲个数 N 在传输过程中被外部截取，保证了门限脉冲个数 N 的安全性； λ 为通信载波信号经过第一终端与第二终端采用的通信协议规定的帧等待时间所产生的脉冲个数变化值，帧等待时间是指通信协议中规定的待处理数据包发出后的有效等待时间，超出帧等待时间后判断通信失败， $N \leq \lambda$ 能够保证第二终端在帧等待时间内将应答数据包发送至第一终端，兼容现有的通信协议，保证在现有通信协议下第一终端与第二终端之间能够进行正常通信。

可选地，第一终端与第二终端基于脉冲通信协议进行数据交互，并基于防篡改校验值对接收到的门限脉冲个数 N 进行校验操作，其中，脉冲通信协议为传输数据中至少包括门限脉冲个数 N 的通信协议；或者，脉冲通信协议为传输数据中至少包括门限脉冲个数 N 和防篡改校验值的通信协议，其中，所示防篡改校验值用于对门限脉冲个数 N 进行校验操作；

第一终端与第二终端采用的通信协议可以规定在通信数据中携带门限脉冲个数 N ，第一

终端与第二终端在通信过程中接收到数据包之后，读取数据包中的门限脉冲个数 N ，并基于数据包中的门限脉冲个数 N 进行计时通信，进一步地，第一终端与第二终端采用的通信协议还可以规定在通信数据中同时携带门限脉冲个数 N 和防篡改校验值，第一终端与第二终端在通信过程中接收到数据包之后，读取数据包中的门限脉冲个数 N 和防篡改校验值，防篡改校验值为基于门限脉冲个数 N 生成的校验值，例如，防篡改校验值为对门限脉冲个数 N 进行摘要运算获得，第一终端与第二终端在通信过程中接收到数据包之后，读取数据包中的门限脉冲个数 N 进行校验操作，一旦第一终端与第二终端在通信过程中接收到数据包之后，读取数据包中的门限脉冲个数 N 被他人篡改，则会导致校验失败，在校验成功后，第一终端与第二终端基于数据包中的门限脉冲个数 N 进行计时通信；可选地，门限脉冲个数 N 与防篡改校验值可以附加于现有通信协议规定的通信数据包的数据头或数据尾，当然，本发明并不限于此；通过将门限脉冲个数 N 写入传输协议，保证每个数据包中均包含有门限脉冲个数 N 信息，第一终端与第二终端无需对门限脉冲个数 N 进行存储，防止第三方攻破第一终端或第二终端的存储模块获得门限脉冲个数 N ，同时提升了通信效率；

门限脉冲个数 N 为第一终端基于 ω 生成，且 $N \geq \omega$ 其中， ω 为通信载波信号经过第二终端对接收到的第一终端发送的数据进行处理的预定完成时间所产生的脉冲个数，

第一终端可以采用多种方式获取 ω ，包括但不限于以下方式： ω 可以为第一终端通过外部按键输入获得、 ω 可以为第二终端发送至第一终端获得、 ω 可以为第一终端扫码获得、 ω 可以为第一终端根据出厂预设信息获得； $N \geq \omega$ 能够保证第二终端在需要发送应答数据包之前，完成对待处理数据包的处理操作并生成应答数据包，保证第一终端与第二终端之间的正常通信得以实现，

可选地， $\omega \leq N \leq \lambda$ ，其中， λ 为通信载波信号经过第一终端与第二终端采用的通信协议规定的帧等待时间所产生的脉冲个数变化值；帧等待时间是指通信协议中规定的待处理数据包发出后的有效等待时间，超出帧等待时间后判断通信失败， $N \leq \lambda$ 能够保证第二终端在帧等待时间内将应答数据包发送至第一终端，兼容现有的通信协议，保证在现有通信协议下第一终端与第二终端之间能够进行正常通信；

第一终端生成门限脉冲个数 N 后，可采用以下方式将门限脉冲个数 N 发送至第二终端：

第一终端利用第二终端公钥加密门限脉冲个数 N ，生成门限脉冲个数密文，并将门限脉冲个数密文发送至第二终端；由于利用第二终端公钥对门限脉冲个数进行加密操作生成的门限脉冲个数密文只能用第二终端私钥进行解密，而第二终端私钥保存在第二终端安全芯片内部，外界无法获得，从而保证了门限脉冲个数 N 的安全性；第二终端接收门限脉冲个数密文，利用第二终端私钥对门限脉冲个数密文进行解密操作，获得门限脉冲个数 N 并存储，实现第一终端将生成的门限脉冲个数 N 发送至第二终端，同时保证了门限脉冲个数 N 发送

过程的安全性；或者，

第一终端生成第一随机数，并将第一随机数与第一终端的 CA 证书发送至第二终端；

第一随机数可以是第一终端根据外部的随机噪声信号生成，也可以是根据内部的随机数生成器生成，保证第一随机数的外部不可获取性；

5 第二终端接收第一随机数与第一终端的 CA 证书，生成第二随机数，对第一终端的 CA 证书进行认证操作，认证成功后，获得第一终端公钥，利用第二终端私钥对第一随机数进行签名操作，生成第一签名信息，利用第一终端公钥对第二随机数进行加密操作，生成第二随机数密文，并将第一协商信息发送至第一终端，其中，第一协商信息至少包括：第二终端的 CA 证书、第一签名信息、第二随机数密文；

10 第二随机数可以是第二终端根据外部的随机噪声信号生成，也可以是根据内部的随机数生成器生成，保证第二随机数的外部不可获取性；第二终端基于第一终端 CA 证书获得第一终端公钥，并利用第一终端公钥对第二随机数进行加密，由于利用第一终端公钥加密生成的第二随机数密文只能用第一终端私钥进行解密，而第一终端私钥保存在第一终端安全芯片内部，外界无法获得，从而保证了第二随机数的安全性；

15 第一终端接收第一协商数据，对第二终端的 CA 证书进行认证操作，认证成功后，基于第二终端公钥对第一签名信息进行验签操作，验签成功后，利用第一设备私钥对第二随机数密文进行解密操作，获得第二随机数，利用第一设备私钥对第二随机数进行签名操作，生成第二签名信息；第一终端生成第三随机数，利用第二设备公钥对第三随机数进行加密，获得第三随机数密文，基于第二随机数与第三随机数根据第一预设算法获得传输密钥，并将第二协商信息发送至第二终端，其中，第二协商信息至少包括：第二签名信息、第三随机数密文；

20 第一终端基于第二终端公钥对第二终端进行身份认证，保证第二终端的合法性，认证成功后，利用自身私钥对第二随机数密文进行解密，获得第二随机数，生成第三随机数，基于第二随机数与第三随机数根据第一预设算法获得传输密钥；第三随机数可以是第一终端根据外部的随机噪声信号生成，也可以是根据内部的随机数生成器生成，保证第三随机数的外部不可获取性；利用第二终端公钥对第三随机数进行加密，由于利用第二终端公钥加密生成的第三随机数密文只能用第二终端私钥进行解密，而第二终端私钥保存在第二终端安全芯片内部，外界无法获得，从而保证了第三随机数的安全性；

25 第二终端接收第二协商数据，基于第一终端公钥对第二签名信息进行验签操作，验签成功后，利用第二终端私钥对第三随机数密文进行解密操作，获得第三随机数，基于第二随机数与第三随机数根据第一预设算法获得传输密钥；第二终端生成传输密钥生成反馈信息，并将传输密钥生成反馈信息发送至第一终端；

第二终端利用自身私钥解密第三随机数密文后，获得第三随机数，基于第二随机数与第

三随机数根据第一预设算法获得传输密钥,由于第一终端与第二终端各自基于第二随机数与第三随机数根据第一预设算法获得传输密钥,既保证了双方协商出同一传输密钥,又无需将传输密钥外发避免了传输密钥在通信过程中外泄,提升了通信的安全性;

第一终端接收传输密钥生成反馈信息,利用传输密钥对生成的门限脉冲个数 N 进行加密,生成门限脉冲个数密文,并将门限脉冲个数密文发送至第二终端;

第一终端利用传输密钥对门限脉冲个数 N 进行加密操作,生成门限脉冲个数密文,由于传输密钥是第一终端与第二终端各自基于第二随机数与第三随机数根据第一预设算法获得,仅存于第一终端与第二终端内部,外界无法获得,从而保证了门限脉冲个数 N 的安全性;

第二终端接收门限脉冲个数密文,利用传输密钥对门限脉冲个数密文进行解密,获得门限脉冲个数 N 并存储;

第二终端利用传输密钥对门限脉冲个数密文进行解密,获得门限脉冲个数 N 并存储,实现第一终端将生成的门限脉冲个数 N 发送至第二终端,同时保证了门限脉冲个数 N 发送过程的安全性。

可选地,门限脉冲个数 N 为第一终端与第二终端协商生成,其中,协商生成包括:第一终端生成 N 并将 N 发送至第二终端,第二终端对第一终端认证成功后向第一终端发送响应信息;或者,第二终端生成 N 并将 N 发送至第一终端,第一终端对第二终端认证成功后向第二终端发送响应信息;或者,第一终端生成 N_1 并将 N_1 发送至第二终端,第二终端生成 N_2 并将 N_2 发送至第一终端,第一终端与第二终端分别基于同样的算法利用 N_1 与 N_2 生成 N ,

上述协商过程可以包括但不限于本实施例提供的以下 3 种实现方案:

方案 1:

第一终端生成第一随机数,并将第一随机数发送至第二终端;

第一随机数可以是第一终端根据外部的随机噪声信号生成,也可以是根据内部的随机数生成器生成,保证第一随机数的外部不可获取性;

第二终端接收第一随机数,生成第二随机数,利用第二设备私钥对第一随机数进行签名操作,生成第一签名信息,并将第一协商数据包发送至第一终端,其中,第一协商数据包至少包括:第二终端的 CA 证书、第一签名信息、第二随机数;

第二随机数可以是第二终端根据外部的随机噪声信号生成,也可以是根据内部的随机数生成器生成,保证第二随机数的外部不可获取性;第二设备基于自身私钥对第一随机数进行签名操作,并将自身 CA 证书发送至第一终端,以使第一终端对自身的合法性进行认证;

第一终端接收第一协商数据,对第二终端的 CA 证书进行认证操作,认证成功后,获得

第二终端公钥，基于第二终端公钥对第一签名信息进行验签操作，验签成功后，利用第一设备私钥对第二随机数进行签名操作，生成第二签名信息，并将第二协商数据包发送至第二终端，其中，第二协商数据包至少包括：第一终端的 CA 证书、第二签名信息；

5 第一终端基于第二终端公钥对第二终端进行身份认证，保证第二终端的合法性，认证成功后，第一设备基于自身私钥对第二随机数进行签名操作，并将自身 CA 证书发送至第二终端，以使第二终端对自身的合法性进行认证；

第二终端接收第二协商数据，对第一终端的 CA 证书进行认证操作，认证成功后，获得第一终端公钥，基于第一终端公钥对第二签名信息进行验签操作，验签成功后，生成门限脉冲个数 N ，利用第一终端公钥对门限脉冲个数 N 进行加密操作，生成门限脉冲个数密文，
10 并将门限脉冲个数密文发送至第一终端；

第二终端基于第一终端公钥对第一终端进行身份认证，保证第一终端的合法性，认证成功后，生成门限脉冲个数 N ，并利用第一终端公钥对门限脉冲个数 N 进行加密操作，生成门限脉冲个数密文，由于利用第一终端公钥对门限脉冲个数 N 进行加密操作生成的门限脉冲个数密文只能用第一终端私钥进行解密，而第一终端私钥保存在第一终端安全芯片内部，
15 外界无法获得，从而保证了门限脉冲个数 N 的安全性。

第一终端接收门限脉冲个数密文，利用第一终端私钥对门限脉冲个数密文进行解密操作，获得门限脉冲个数 N 并存储；

第一终端利用自身私钥对门限脉冲个数密文进行解密，获得门限脉冲个数 N 并存储，实现第一终端与第二终端之间的门限脉冲个数 N 的协商，同时保证了协商过程的安全性。

20 方案 2：

第一终端生成第一随机数，并将第一随机数与第一终端的 CA 证书发送至第二终端；

第一随机数可以是第一终端根据外部的随机噪声信号生成，也可以是根据内部的随机数生成器生成，保证第一随机数的外部不可获取性；

第二终端接收第一随机数与第一终端的 CA 证书，生成第二随机数，对第一终端的 CA
25 证书进行认证操作，认证成功后，获得第一终端公钥，利用第二终端私钥对第一随机数进行签名操作，生成第一签名信息，利用第一终端公钥对第二随机数进行加密操作，生成第二随机数密文，并将第一协商信息发送至第一终端，其中，第一协商信息至少包括：第二终端的 CA 证书、第一签名信息、第二随机数密文；

第二随机数可以是第二终端根据外部的随机噪声信号生成，也可以是根据内部的随机数
30 生成器生成，保证第二随机数的外部不可获取性；第二终端基于第一终端 CA 证书获得第一终端公钥，并利用第一终端公钥对第二随机数进行加密，由于利用第一终端公钥加密生成的第二随机数密文只能用第一终端私钥进行解密，而第一终端私钥保存在第一终端安全芯片内

部，外界无法获得，从而保证了第二随机数的安全性；

第一终端接收第一协商数据，对第二终端的 CA 证书进行认证操作，认证成功后，基于第二终端公钥对第一签名信息进行验签操作，验签成功后，利用第一设备私钥对第二随机数密文进行解密操作，获得第二随机数，利用第一设备私钥对第二随机数进行签名操作，生成第二签名信息；第一终端生成第三随机数，利用第二设备公钥对第三随机数进行加密，获得第三随机数密文，基于第二随机数与第三随机数根据第一预设算法获得传输密钥，并将第二协商信息发送至第二终端，其中，第二协商信息至少包括：第二签名信息、第三随机数密文；

第一终端基于第二终端公钥对第二终端进行身份认证，保证第二终端的合法性，认证成功后，利用自身私钥对第二随机数密文进行解密，获得第二随机数，生成第三随机数，基于第二随机数与第三随机数根据第一预设算法获得传输密钥；第三随机数可以是第一终端根据外部的随机噪声信号生成，也可以是根据内部的随机数生成器生成，保证第三随机数的外部不可获取性；利用第二终端公钥对第三随机数进行加密，由于利用第二终端公钥加密生成的第三随机数密文只能用第二终端私钥进行解密，而第二终端私钥保存在第二终端安全芯片内部，外界无法获得，从而保证了第三随机数的安全性；

第二终端接收第二协商数据，基于第一终端公钥对第二签名信息进行验签操作，验签成功后，利用第二终端私钥对第三随机数密文进行解密操作，获得第三随机数，基于第二随机数与第三随机数根据第一预设算法获得传输密钥；第二终端生成传输密钥生成反馈信息，并将传输密钥生成反馈信息发送至第一终端；

第二终端利用自身私钥解密第三随机数密文后，获得第三随机数，基于第二随机数与第三随机数根据第一预设算法获得传输密钥，由于第一终端与第二终端各自基于第二随机数与第三随机数根据第一预设算法获得传输密钥，既保证了双方协商出同一传输密钥，又无需将传输密钥外发避免了传输密钥在通信过程中外泄，提升了通信的安全性；

第一终端接收传输密钥生成反馈信息，生成门限脉冲个数 N ，利用传输密钥对门限脉冲个数 N 进行加密，生成门限脉冲个数密文，并将门限脉冲个数密文发送至第二终端；

第一终端生成门限脉冲个数 N ，并利用传输密钥对门限脉冲个数 N 进行加密操作，生成门限脉冲个数密文，由于传输密钥是第一终端与第二终端各自基于第二随机数与第三随机数根据第一预设算法获得，仅存于第一终端与第二终端内部，外界无法获得，从而保证了门限脉冲个数 N 的安全性；

第二终端接收门限脉冲个数密文，利用传输密钥对门限脉冲个数密文进行解密，获得门限脉冲个数 N 并存储；

第二终端利用传输密钥对门限脉冲个数密文进行解密，获得门限脉冲个数 N 并存储，实现第一终端与第二终端之间的门限脉冲个数 N 协商，同时保证了协商过程的安全性。

方案 3:

第一终端生成第一随机数, 并将第一随机数与第一终端的 CA 证书发送至第二终端;

第一随机数可以是第一终端根据外部的随机噪声信号生成, 也可以是根据内部的随机数生成器生成, 保证第一随机数的外部不可获取性;

5 第二终端接收第一随机数与第一终端的 CA 证书, 生成 N2, 对第一终端的 CA 证书进行认证操作, 认证成功后, 获得第一终端公钥, 利用第二终端私钥对第一随机数进行签名操作, 生成第一签名信息, 利用第一终端公钥对 N2 进行加密操作, 生成 N2 密文, 并将第一协商信息发送至第一终端, 其中, 第一协商信息至少包括: 第二终端的 CA 证书、第一签名信息、N2 密文;

10 N2 可以是第二终端根据外部的随机噪声信号生成, 也可以是根据内部的随机数生成器生成, 保证 N2 的外部不可获取性; 第二终端基于第一终端 CA 证书获得第一终端公钥, 并利用第一终端公钥对 N2 进行加密, 由于利用第一终端公钥加密生成的 N2 密文只能用第一终端私钥进行解密, 而第一终端私钥保存在第一终端安全芯片内部, 外界无法获得, 从而保证了 N2 的安全性;

15 第一终端接收第一协商数据, 对第二终端的 CA 证书进行认证操作, 认证成功后, 基于第二终端公钥对第一签名信息进行验签操作, 验签成功后, 利用第一设备私钥对 N2 密文进行解密操作, 获得 N2, 利用第一设备私钥对 N2 进行签名操作, 生成第二签名信息; 第一终端生成 N1, 利用第二设备公钥对 N1 进行加密, 获得 N1 密文, 基于 N1 与 N2 根据第二预设算法生成门限脉冲个数 N, 并将第二协商信息发送至第二终端, 其中, 第二协商信息至少包括: 第二签名信息、N1 密文;

20 第一终端基于第二终端公钥对第二终端进行身份认证, 保证第二终端的合法性, 认证成功后, 利用自身私钥对 N2 密文进行解密, 获得 N2, 生成 N1, 基于 N1 与 N2 根据第二预设算法获得门限脉冲个数 N; N1 可以是第一终端根据外部的随机噪声信号生成, 也可以是根据内部的随机数生成器生成, 保证 N1 的外部不可获取性; 利用第二终端公钥对 N1 进行加密, 由于利用第二终端公钥加密生成的 N1 密文只能用第二终端私钥进行解密, 而第二终端私钥保存在第二终端安全芯片内部, 外界无法获得, 从而保证了 N1 的安全性;

第二终端接收第二协商数据, 基于第一终端公钥对第二签名信息进行验签操作, 验签成功后, 利用第二终端私钥对 N1 密文进行解密操作, 获得 N1, 基于 N1 与 N2 根据第二预设算法获得门限脉冲个数 N;

30 第二终端利用自身私钥解密 N1 密文后, 获得 N1, 基于 N1 与 N2 根据第二预设算法获得门限脉冲个数 N, 由于第一终端与第二终端各自基于 N1 与 N2 根据第二预设算法获得门限脉冲个数 N, 既保证了双方协商出同一门限脉冲个数 N, 又无需将门限脉冲个数 N 外发避

免了门限脉冲个数 N 在通信过程中外泄，提升了通信的安全性。

通过上述门限脉冲个数 N 的协商过程，能够保证门限脉冲个数 N 生成的安全性，避免门限脉冲个数 N 被外部获取，进一步地，上述门限脉冲个数 N 的协商过程可以在每次信息交互之前重新协商生成，从而进一步保证门限脉冲个数 N 的安全性。

5 可选地，第一终端与第二终端采用的通信方式包括：短距离无线通信方式，其中，短距离无线通信方式可以包括以下通信协议：蓝牙通信协议、红外 IrDA 通信协议、RFID 通信协议、ZigBee 通信协议、超宽频(Ultra WideBand) 通信协议、短距通信(NFC) 通信协议、WiMedia 通信协议、GPS 通信协议、DECT 通信协议、无线 1394 通信协议和专用无线通信协议，当然，未来有可能出现的以下通信协议等同于上述通信协议：通信协议支持的最大传输距离下
10 数据传播所需时间小于数据被外部设备篡改所需时间。

根据上述内容可知，通过本实施例提供的数据通信方法，第一终端发送完毕待处理数据包时开始记录第一终端发送的通信载波信号的第一终端脉冲个数，并仅在第一终端脉冲个数符合门限范围时接收应答数据包；第二终端接收完毕开始记录第二终端接收到的通信载波信号的第二终端脉冲个数，并仅在第二终端脉冲个数达到 N 时发送应答数据包，第一终端与
15 第二终端通过检测脉冲个数进行同时收发数据，大大提升了双方计时的精确度，从而保证了第一终端和第二终端仅在特定的高精度时刻收发应答数据包，即使第二终端向第一终端发送的应答数据包在传输过程中被第三方截获，由于第三方对数据的篡改时间为毫秒级别，远远大于第一终端的计时精度，第一终端在特定时刻未接收到应答数据包立即停止通信流程，第三方篡改后的数据到达第一终端时，第一终端已终止通信流程，从而杜绝了第一终端接收到的
20 的数据在传输过程中被外界篡改的风险，大大提升了第一终端接收到的应答数据包的可靠性，此外， $N \geq \omega$ 能够保证第二终端在需要发送应答数据包之前完成对待处理数据包的处理操作并生成应答数据包， $N \leq \lambda$ 能够使本通信方法和系统兼容现有的通信协议。

本实施例提供一种数据通信系统，如图 3 所示，用于执行图 1 或 2 示出的方法实施例中的安全通信方法，该系统包括：第一终端和第二终端。

25 所述第一终端，用于发送携带有待处理数据包的通信数据信号，在所述第一终端发送完毕所述待处理数据包时开始记录所述第一终端发送的所述通信载波信号的第一终端脉冲个数；所述通信数据信号由所述第一终端将所述待处理数据包调制在所述通信载波信号上得到；所述第二终端，用于接收携带有所述待处理数据包的所述通信数据信号，在所述第二终端接收完毕所述待处理数据包时开始记录所述第二终端接收到的所述通信载波信号的第二
30 终端脉冲个数，并基于所述待处理数据包生成应答数据包；所述第二终端，用于在记录所述第二终端脉冲个数达到门限脉冲个数 N 时，将所述应答数据包发送至所述第一终端；所述第一终端，用于在记录所述第一终端脉冲个数达到所述门限脉冲个数 N 时，允许开始接收

所述应答数据包。

可选地，所述第一终端，还用于生成通信请求，并将所述通信请求发送至所述第二终端；所述第二终端，还用于接收所述通信请求，基于所述通信请求生成第一协商数据包，并将所述第一协商数据包发送至所述第一终端；所述第一终端，还用于接收所述第一协商数据，基于所述
5 所述第一协商数据对所述第二终端进行认证操作，认证成功后，生成第二协商数据包，并将所述第二协商数据包发送至所述第二终端；所述第二终端，还用于接收所述第二协商数据包，基于所述第二协商数据包对所述第一终端进行认证操作，认证成功后，生成所述门限脉冲个数 N ，对所述门限脉冲个数 N 进行加密操作，生成门限脉冲个数密文，并将所述门限脉冲个数密文发送至所述第一终端，其中，所述 $N \leq \lambda$ ，所述 λ 为所述通信载波信号经过所述
10 所述第一终端与所述第二终端采用的通信协议规定的帧等待时间所产生的脉冲个数；所述第一终端，还用于接收所述门限脉冲个数密文，对所述门限脉冲个数密文进行解密操作，获得所述门限脉冲个数 N 并存储。

可选地，所述第一终端与所述第二终端的出厂预置信息中存储有所述门限脉冲个数 N ，其中，所述 $N \leq \lambda$ ，所述 λ 为所述通信载波信号经过所述第一终端与所述第二终端采用的通
15 信协议规定的帧等待时间所产生的脉冲个数。

可选地，所述第一终端与所述第二终端基于脉冲通信协议进行数据交互，并基于防篡改校验值对接收到的所述门限脉冲个数 N 进行校验操作，其中，所述脉冲通信协议为传输数据中至少包括所述门限脉冲个数 N 和所述防篡改校验值的通信协议；所述门限脉冲个数 N 为所述第一终端基于 ω 生成，且 $N \geq \omega$ 其中，所述 ω 为所述通信载波信号经过所述第二终端
20 对接收到的所述第一终端发送的数据进行处理的预定完成时间所产生的脉冲个数，或，所述门限脉冲个数 N 为所述第一终端与所述第二终端协商生成，其中，所述协商生成包括：所述第一终端生成所述 N 并将所述 N 发送至所述第二终端，所述第二终端对所述第一终端认证成功后向所述第一终端发送响应信息；或者，所述第二终端生成所述 N 并将所述 N 发送至所述第一终端，所述第一终端对所述第二终端认证成功后向所述第二终端发送响应信息；
25 或者，所述第一终端生成 $N1$ 并将所述 $N1$ 发送至所述第二终端，所述第二终端生成 $N2$ 并将所述 $N2$ 发送至所述第一终端，所述第一终端与所述第二终端分别基于同样的算法利用所述 $N1$ 与所述 $N2$ 生成所述 N 。

可选地，所述第一终端与所述第二终端采用的通信方式包括：短距离无线通信方式。

由上述本发明提供的技术方案可以看出，本发明提供了一种数据通信方法与一种数据通信系统，第一终端发送完毕待处理数据包时开始记录第一终端发送的通信载波信号的第一终端脉冲个数，并仅在第一终端脉冲个数达到门限脉冲个数 N 时接收应答数据包；第二终端接收完毕开始记录第二终端接收到的通信载波信号的第二终端脉冲个数，并仅在第二终端脉
30

冲个数达到 N 时发送应答数据包，第一终端与第二终端通过检测脉冲个数进行同时收发数据，大大提升了双方计时的精确度，从而保证了第一终端和第二终端仅在特定的高精度时刻收发应答数据包，即使第二终端向第一终端发送的应答数据包在传输过程中被第三方截获，由于第三方对数据的篡改时间为毫秒级别，远远大于第一终端的计时精度，第一终端在特定时刻未接收到应答数据包立即停止通信流程，第三方篡改后的数据到达第一终端时，第一终端已终止通信流程，从而杜绝了第一终端接收到的数据在传输过程中被外界篡改的风险，大大提升了第一终端接收到的应答数据包的可靠性，此外， $N \geq \omega$ 能够保证第二终端在需要发送应答数据包之前完成对待处理数据包的处理操作并生成应答数据包， $N \leq \lambda$ 能够使本通信方法和系统兼容现有的通信协议。

实施例 2

本实施例提供一种数据通信方法，如附图 4 所示，包括以下步骤：

S401，第一终端发送携带有待处理数据包的通信数据信号，

S402，在第一终端发送完毕待处理数据包时开始记录第一终端发送的通信载波信号的第一终端脉冲个数；通信数据信号由第一终端将待处理数据包调制在通信载波信号上得到；

S403，第二终端接收携带有待处理数据包的通信数据信号，

S404，在第二终端接收完毕待处理数据包时开始记录第二终端接收到的通信载波信号的第二终端脉冲个数，并基于待处理数据包生成应答数据包；

S405，第二终端在记录第二终端脉冲个数达到门限脉冲个数 N 时，将应答数据包发送至第一终端；

上述步骤 S401 至 S405 还可以参见实施例 1 中步骤 S101 至 S105 中的相关描述。

S406，第一终端记录第一终端脉冲个数在门限范围内，允许开始接收应答数据包；

在实际通信过程中，由于第一终端和第二终端存在数据传输时间、数据接收时间、数据分析处理时间、数据纠错时间等各种通信时间，第一终端并不一定能够在检测到第一脉冲个数到达 N 时立刻接收到应答数据包，实际上，在正常通信状态下，第一终端接收到第二终端在检测到第二脉冲个数达到门限脉冲个数 N 时外发的应答数据包时，第一终端检测到的第一脉冲个数值为 $N+i$ ， i 为通信载波信号经过数据传输时间、数据接收时间、数据分析处理时间、数据纠错时间等各种通信时间后产生的脉冲个数变化值，因此，第一终端并不能够在检测到第一脉冲个数到达 N 时立刻接收到应答数据包，而是在检测到第一脉冲个数到达 N 后的一个很小的时间范围内接收到应答数据包，基于门限脉冲个数 N 根据误差算法可以得到一个门限范围，在该门限范围仅能够实现第一终端和第二终端之间的最大数据传输时间、最大数据接收时间、最大数据分析处理时间、最大数据纠错时间等最大通信时间，由于在实

际通信过程中, 第一终端和第二终端之间的最大数据传输时间、最大数据接收时间、最大数据分析处理时间、最大数据纠错时间等最大通信时间的实际数值均为极小值, 因此根据误差算法获得的门限范围是一个很小的脉冲个数范围, 例如,

在第一终端检测到第一脉冲个数到达 N 之前拒绝接收数据, 当第一终端检测到第一脉冲个数到达 N 时, 开始允许开始接收应答数据包, 当第一终端检测到第一脉冲个数到达 $N+2\theta$ 时, 开始拒绝接收应答数据包, 由于第一终端与第二终端之间存在一定的通信距离 S , 通信载波信号经过通信距离 S 后会产生一定量的脉冲变化值 ε , 第一终端并不一定能够在检测到第一脉冲个数到达 N 时立刻接收到应答数据包, 实际上, 在正常通信状态下, 第一终端接收到第二终端在检测到第二脉冲个数达到门限脉冲个数 N 时外发的应答数据包时, 第一终端检测到的第一脉冲个数为 $N+2\varepsilon$, 由于第一终端与第二终端之间的实际通信距离 S 必然小于第一终端与第二终端采用的通信方式支持的最大通信距离, 可选地, 第一终端与第二终端采用的通信方式包括: 短距离无线通信方式, 而 n 为通信载波信号经过第一终端与第二终端采用的通信方式支持的最大通信距离所产生的脉冲个数变化值, 那么 ε 必然小于 n , 也就是说, 正常通信状态下, 第一终端检测到第一脉冲个数在 $[N, N+2n]$ 范围内时, 必然能够接收到应答数据包, 一旦第一终端检测到的第一脉冲个数超过 $N+2n$ 且未接收到应答数据包, 可以判定应答数据包传输异常, 拒绝接收应答数据包, 从而保证通信的安全性; 可选地, $N+2n$ 小于或等于 λ , 所述 λ 为所述通信载波信号经过所述第一终端与所述第二终端采用的通信协议规定的帧等待时间所产生的脉冲个数, $N+2n$ 小于或等于 λ 能够保证第一终端在帧等待时间内将应答数据包发送至第二终端, 兼容现有的通信协议, 保证在现有通信协议下第一终端与第二终端之间能够进行正常通信; 当 $N+2n$ 小于或等于 λ 时, N 也必然小于 λ , 能够保证第二终端在帧等待时间内将应答数据包发送至第一终端, 兼容现有的通信协议, 保证在现有通信协议下第一终端与第二终端之间能够进行正常通信;

例如, 当第一终端与第二终端距离小于 10 厘米时, 由于数据信号以光速传播, 此时传播所需的时间可以忽略不计, 也就是说, 第一终端接收到第二终端在检测到第二脉冲个数达到门限脉冲个数 N 时外发的应答数据包时, 第一终端检测到的第一脉冲个数同样为 N , 此时由于 N 处于 $[N, N+2n]$ 范围内, 第一终端允许开始接收数据直至接收完毕, 并对接收完毕的数据进行处理, 可见在本实施例中, 第一终端与第二终端距离极小时, 能够保证正常通信; 当第一终端与第二终端距离为通信方式支持的最大通信距离时, 例如蓝牙 2.0 最大支持 10 米的通信距离、zigbee 最大支持 400 米的通信距离, 此时通信载波信号经过第一终端与第二终端之间的空间区域后所产生的脉冲个数变化值为 n , 也就是说, 第一终端接收到第二终端在检测到第二脉冲个数达到门限脉冲个数 N 时外发的应答数据包时, 第一终端检测到的第一脉冲个数为 $N+2n$, 此时由于 $N+2n$ 处于 $[N, N+2n]$ 范围内, 第一终端允许开始接收数据直

至接收完毕，并对接收完毕的数据进行处理，可见在本实施例中，第一终端与第二终端距离为通信方式支持的最大距离时，也能够保证正常通信；当第一终端与第二终端距离处于通信方式支持的最大通信距离内时，通信载波信号经过第一终端与第二终端之间的空间区域后所产生的脉冲个数变化值为 ε ，且 ε 小于 n ，第一终端接收到第二终端在检测到第二脉冲个数达到门限脉冲个数 N 时外发的应答数据包时，第一终端检测到的第一脉冲个数为 $N+2\varepsilon$ ，此时由于 $N+2\varepsilon$ 处于 $[N, N+2n]$ 范围内，第一终端允许开始接收数据直至接收完毕，并对接收完毕的数据进行处理，可见在本实施例中，第一终端与第二终端距离为通信方式支持的最大距离时，同样能够保证正常通信；除去上述情形外，第一终端不允许接收外部发送的数据信息，也就是说，第一终端仅在检测到的第一脉冲个数在 $[N, N+2n]$ 范围内时，才允许开始接收应答数据包，大大提升了接收到的应答数据包的可靠性。本实施例中，第一终端与第二终端可以为能够进行数据交互通信的任意设备，可选地，第一终端可以为读取器，该读取器可以为读卡器、计算机、手机、路由器、车载设备、服务器等设备，第二终端可以为应答器，该应答器可以为智能卡、身份证、智能密钥设备、手机、计算机、路由器、智能家居、可穿戴设备等设备，在数据通信过程中，第一终端与第二终端通过检测脉冲个数进行同时收发大大提升了双方计时的精确度，从而保证了第一终端和第二终端仅在特定的高精度时刻收发应答数据包，即使第二终端向第一终端发送的应答数据包在传输过程中被第三方截获，由于第三方对数据的篡改时间为毫秒级别，远远大于第一终端的计时精度，第一终端在特定时刻未接收到应答数据包立即停止通信流程，第三方篡改后的数据到达第一终端时，第一终端已终止通信流程，从而杜绝了第一终端接收到的数据在传输过程中被外界篡改的风险，大大提升了第一终端接收到的应答数据包的可靠性。

可选地，在步骤 S401 第一终端发送携带有待处理数据包的通信数据信号之前，还包括门限脉冲个数协商方法中的步骤，具体参见上述实施例 1 中图 2 所示方法的具体描述。

本实施例提供一种数据通信系统，用于执行图 4 示出的方法实施例中的安全通信方法，该系统包括：第一终端和第二终端。

第一终端，用于发送携带有待处理数据包的通信数据信号，在第一终端发送完毕待处理数据包时开始记录第一终端发送的通信载波信号的第一终端脉冲个数；通信数据信号由第一终端将待处理数据包调制在通信载波信号上得到；第二终端，用于接收携带有待处理数据包的通信数据信号，在第二终端接收完毕待处理数据包时开始记录第二终端接收到的通信载波信号的第二终端脉冲个数，并基于待处理数据包生成应答数据包；第二终端在检测到第二终端脉冲个数达到门限脉冲个数 N 时，将应答数据包发送至第一终端；第一终端在检测到第一终端脉冲个数在门限范围内时，允许开始接收应答数据包，其中，门限范围为第一终端基于门限脉冲个数 N 获得。

可选地，第一终端，还用于生成通信请求，并将通信请求发送至第二终端；第二终端，还用于接收通信请求，基于通信请求生成第一协商数据包，并将第一协商数据包发送至第一终端；第一终端，还用于接收第一协商数据，基于第一协商数据对第二终端进行认证操作，认证成功后，生成第二协商数据包，并将第二协商数据包发送至第二终端；第二终端，还用于接收第二协商数据包，基于第二协商数据包对第一终端进行认证操作，认证成功后，生成门限脉冲个数 N ，对门限脉冲个数 N 进行加密操作，生成门限脉冲个数密文，并将门限脉冲个数密文发送至第一终端，其中， $N \leq \lambda$ ， λ 为通信载波信号经过第一终端与第二终端采用的通信协议规定的帧等待时间所产生的脉冲个数；第一终端，还用于接收门限脉冲个数密文，对门限脉冲个数密文进行解密操作，获得门限脉冲个数 N 并存储。

可选地，第一终端与第二终端的出厂预置信息中存储有门限脉冲个数 N ，其中， $N \leq \lambda$ ， λ 为通信载波信号经过第一终端与第二终端采用的通信协议规定的帧等待时间所产生的脉冲个数。

可选地，第一终端与第二终端基于脉冲通信协议进行数据交互，并基于防篡改校验值对接收到的门限脉冲个数 N 进行校验操作，其中，脉冲通信协议为传输数据中至少包括门限脉冲个数 N 的通信协议；或者，脉冲通信协议为传输数据中至少包括门限脉冲个数 N 和防篡改校验值的通信协议，其中，所示防篡改校验值用于对门限脉冲个数 N 进行校验操作；门限脉冲个数 N 为第一终端基于 ω 生成，且 $N \geq \omega$ 其中， ω 为通信载波信号经过第二终端对接收到的第一终端发送的数据进行处理的预定完成时间所产生的脉冲个数，或，门限脉冲个数 N 为第一终端与第二终端协商生成，其中，协商生成包括：第一终端生成 N 并将 N 发送至第二终端，第二终端对第一终端认证成功后向第一终端发送响应信息；或者，第二终端生成 N 并将 N 发送至第一终端，第一终端对第二终端认证成功后向第二终端发送响应信息；或者，第一终端生成 $N1$ 并将 $N1$ 发送至第二终端，第二终端生成 $N2$ 并将 $N2$ 发送至第一终端，第一终端与第二终端分别基于同样的算法利用 $N1$ 与 $N2$ 生成 N 。

可选地，第一终端与第二终端采用的通信方式包括：短距离无线通信方式。

可选地，门限范围为 $[N, N+2n]$ ，其中，所述 n 为所述通信载波信号经过所述第一终端与所述第二终端采用的通信方式规定的最大通信距离所产生的脉冲个数。

由上述本发明提供的技术方案可以看出，本发明提供了一种数据通信方法与一种数据通信系统，第一终端发送完毕待处理数据包时开始记录第一终端发送的通信载波信号的第一终端脉冲个数，并仅在第一终端脉冲个数符合门限范围时接收应答数据包；第二终端接收完毕开始记录第二终端接收到的通信载波信号的第二终端脉冲个数，并仅在第二终端脉冲个数达到 N 时发送应答数据包，第一终端与第二终端通过检测脉冲个数进行同时收发数据，大大提升了双方计时的精确度，从而保证了第一终端和第二终端仅在特定的高精度时刻收发应答

数据包，即使第二终端向第一终端发送的应答数据包在传输过程中被第三方截获，由于第三方对数据的篡改时间为毫秒级别，远远大于第一终端的计时精度，第一终端在特定时刻未接收到应答数据包立即停止通信流程，第三方篡改后的数据到达第一终端时，第一终端已终止通信流程，从而杜绝了第一终端接收到的数据在传输过程中被外界篡改的风险，大大提升了第一终端接收到的应答数据包的可靠性，此外， $N \geq \omega$ 能够保证第二终端在需要发送应答数据包之前完成对待处理数据包的处理操作并生成应答数据包， $N \leq \lambda$ 能够使本通信方法和系统兼容现有的通信协议。

本实施例 2 仅对与实施例 1 相区别的部分进行详细描述，其余相似部分不再赘述，具体可以参见实施例 1 中的相关描述。

流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的组件、片段或部分，并且本发明的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本发明的实施例所属技术领域的技术人员所理解。

应当理解，本发明的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如，如果用硬件来实现，和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现：具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列（PGA），现场可编程门阵列（FPGA）等。

本技术领域的普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，该程序在执行时，包括方法实施例的步骤之一或其组合。

此外，在本发明各个实施例中的各功能单元可以集成在一个处理组件中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个组件中。上述集成的组件既可以采用硬件的形式实现，也可以采用软件功能组件的形式实现。所述集成的组件如果以软件功能组件的形式实现并作为独立的产品销售或使用，也可以存储在一个计算机可读取存储介质中。

上述提到的存储介质可以是只读存储器，磁盘或光盘等。

在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含

于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

- 5 尽管上面已经示出和描述了本发明的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本发明的限制，本领域的普通技术人员在不脱离本发明的原理和宗旨的情况下在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。本发明的范围由所附权利要求及其等同限定。

权 利 要 求 书

1、一种数据通信方法，其特征在于，在第一终端与第二终端通信过程中，所述第一终端始终产生通信载波信号，所述方法包括以下步骤：

5 所述第一终端发送携带有待处理数据包的通信数据信号，在所述第一终端发送完毕所述待处理数据包时开始记录所述第一终端发送的所述通信载波信号的第一终端脉冲个数；所述通信数据信号由所述第一终端将所述待处理数据包调制在所述通信载波信号上得到；

所述第二终端接收携带有所述待处理数据包的所述通信数据信号，在所述第二终端接收完毕所述待处理数据包时开始记录所述第二终端接收到的所述通信载波信号的第二终端脉冲个数，并基于所述待处理数据包生成应答数据包；

所述第二终端在记录所述第二终端脉冲个数达到门限脉冲个数 N 时，将所述应答数据包发送至所述第一终端；

所述第一终端记录所述第一终端脉冲个数达到所述门限脉冲个数 N 时，允许开始接收所述应答数据包。

15 2、根据权利要求 1 所述的方法，其特征在于，在所述第一终端发送携带有所述待处理数据包的所述通信数据信号之前，还包括步骤：

所述第一终端生成通信请求，并将所述通信请求发送至所述第二终端；

所述第二终端接收所述通信请求，基于所述通信请求生成第一协商数据包，并将所述第一协商数据包发送至所述第一终端；

20 所述第一终端接收所述第一协商数据，基于所述第一协商数据对所述第二终端进行认证操作，认证成功后，生成第二协商数据包，并将所述第二协商数据包发送至所述第二终端；

所述第二终端接收所述第二协商数据包，基于所述第二协商数据包对所述第一终端进行认证操作，认证成功后，生成所述门限脉冲个数 N ，对所述门限脉冲个数 N 进行加密操作，生成门限脉冲个数密文，并将所述门限脉冲个数密文发送至所述第一终端，其中，所述 $N \leq \lambda$ ，所述 λ 为所述通信载波信号经过所述第一终端与所述第二终端采用的通信协议规定的帧等待时间所产生的脉冲个数；

所述第一终端接收所述门限脉冲个数密文，对所述门限脉冲个数密文进行解密操作，获得所述门限脉冲个数 N 并存储。

30 3、根据权利要求 1 所述的方法，其特征在于，所述第一终端与所述第二终端的出厂预置信息中存储有所述门限脉冲个数 N ，其中，所述 $N \leq \lambda$ ，所述 λ 为所述通信载波信号经过所述第一终端与所述第二终端采用的通信协议规定的帧等待时间所产生的脉

冲个数。

4、根据权利要求 1 所述的方法，其特征在于，所述第一终端与所述第二终端基于脉冲通信协议进行数据交互，并基于防篡改校验值对接收到的所述门限脉冲个数 N 进行校验操作，其中，所述脉冲通信协议为传输数据中至少包括所述门限脉冲个数 N 和所述防篡改校验值的通信协议；

所述门限脉冲个数 N 为所述第一终端基于 ω 生成，且 $N \geq \omega$ 其中，所述 ω 为所述通信载波信号经过所述第二终端对接收到的所述第一终端发送的数据进行处理的预定完成时间所产生的脉冲个数，或，

所述门限脉冲个数 N 为所述第一终端与所述第二终端协商生成，其中，所述协商生成包括：所述第一终端生成所述 N 并将所述 N 发送至所述第二终端，所述第二终端对所述第一终端认证成功后向所述第一终端发送响应信息；或者，所述第二终端生成所述 N 并将所述 N 发送至所述第一终端，所述第一终端对所述第二终端认证成功后向所述第二终端发送响应信息；或者，所述第一终端生成 $N1$ 并将所述 $N1$ 发送至所述第二终端，所述第二终端生成 $N2$ 并将所述 $N2$ 发送至所述第一终端，所述第一终端与所述第二终端分别基于同样的算法利用所述 $N1$ 与所述 $N2$ 生成所述 N 。

5、根据权利要求 1 至 3 任一项所述的方法，其特征在于，所述第一终端与所述第二终端采用的通信方式包括：短距离无线通信方式；

所述第一终端为读取器，所述第二终端为应答器。

6、一种数据通信系统，至少包括权利要求 1-5 任一项所述方法中的所述第一终端和所述第二终端，所述第一终端和所述第二终端执行权利要求 1-5 任一项所述的方法。

7、一种数据通信方法，其特征在于，在第一终端与第二终端通信过程中，所述第一终端始终产生通信载波信号，所述方法包括以下步骤：

所述第一终端发送携带有待处理数据包的通信数据信号，在所述第一终端发送完毕所述待处理数据包时开始记录所述第一终端发送的所述通信载波信号的第一终端脉冲个数；所述通信数据信号由所述第一终端将所述待处理数据包调制在所述通信载波信号上得到；

所述第二终端接收携带有所述待处理数据包的所述通信数据信号，在所述第二终端接收完毕所述待处理数据包时开始记录所述第二终端接收到的所述通信载波信号的第二终端脉冲个数，并基于所述待处理数据包生成应答数据包；

所述第二终端在检测到所述第二终端脉冲个数达到门限脉冲个数 N 时，将所述应答数据包发送至所述第一终端；

所述第一终端在检测到所述第一终端脉冲个数在门限范围内时，允许开始接收所述

应答数据包，其中，所述门限范围为所述第一终端基于所述门限脉冲个数 N 获得。

8、根据权利要求 7 所述的方法，其特征在于，在所述第一终端发送携带有所述待处理数据包的所述通信数据信号之前，还包括步骤：

所述第一终端生成通信请求，并将所述通信请求发送至所述第二终端；

5 所述所述第二终端接收所述通信请求，基于所述通信请求生成第一协商数据包，并将所述第一协商数据包发送至所述第一终端；

所述第一终端接收所述第一协商数据，基于所述第一协商数据对所述第二终端进行认证操作，认证成功后，生成第二协商数据包，并将所述第二协商数据包发送至所述第二终端；

10 所述所述第二终端接收所述第二协商数据包，基于所述第二协商数据包对所述第一终端进行认证操作，认证成功后，生成所述门限脉冲个数 N ，对所述门限脉冲个数 N 进行加密操作，生成门限脉冲个数密文，并将所述门限脉冲个数密文发送至所述第一终端，其中，所述 $N \leq \lambda$ ，所述 λ 为所述通信载波信号经过所述第一终端与所述第二终端采用的通信协议规定的帧等待时间所产生的脉冲个数；

15 所述第一终端接收所述门限脉冲个数密文，对所述门限脉冲个数密文进行解密操作，获得所述门限脉冲个数 N 并存储。

9、根据权利要求 7 所述的方法，其特征在于，所述第一终端与所述第二终端的出厂预置信息中存储有所述门限脉冲个数 N ，其中，所述 $N \leq \lambda$ ，所述 λ 为所述通信载波信号经过所述第一终端与所述第二终端采用的通信协议规定的帧等待时间所产生的脉
20 冲个数。

10、根据权利要求 7 所述的方法，其特征在于，所述第一终端与所述第二终端基于脉冲通信协议进行数据交互，并基于防篡改校验值对接收到的所述门限脉冲个数 N 进行校验操作，其中，所述脉冲通信协议为传输数据中至少包括所述门限脉冲个数 N 的通信协议；或者，所述脉冲通信协议为传输数据中至少包括所述门限脉冲个数 N 和所述防篡改校验值的通信协议，其中，所述防篡改校验值用于对所述门限脉冲个数 N 进行校验操
25 作；

所述门限脉冲个数 N 为所述第一终端基于 ω 生成，且 $N \geq \omega$ 其中，所述 ω 为所述通信载波信号经过所述第二终端对接收到的所述第一终端发送的数据进行处理的预定完成时间所产生的脉冲个数，或，

30 所述门限脉冲个数 N 为所述第一终端与所述第二终端协商生成，其中，所述协商生成包括：所述第一终端生成所述 N 并将所述 N 发送至所述第二终端，所述第二终端对所述第一终端认证成功后向所述第一终端发送响应信息；或者，所述第二终端生成所述

N 并将所述 N 发送至所述第一终端，所述第一终端对所述第二终端认证成功后向所述第二终端发送响应信息；或者，所述第一终端生成 N1 并将所述 N1 发送至所述第二终端，所述第二终端生成 N2 并将所述 N2 发送至所述第一终端，所述第一终端与所述第二终端分别基于同样的算法利用所述 N1 与所述 N2 生成所述 N。

5 11、根据权利要求 7 至 6 任一项所述的方法，其特征在于，所述第一终端与所述第二终端采用的所述通信方式包括：短距离无线通信方式；所述第一终端为读取器，所述第二终端为应答器。

12、根据权利要求 7 至 10 任一项所述的方法，其特征在于，所述门限范围为 $[N, N+2n]$ ，其中， $N+2n$ 小于或等于 λ ，所述 λ 为所述通信载波信号经过所述第一终端与
10 所述第二终端采用的通信协议规定的帧等待时间所产生的脉冲个数，所述 n 为所述通信载波信号经过所述第一终端与所述第二终端采用的通信方式规定的最大通信距离所产生的脉冲个数。

13、一种数据通信系统，至少包括权利要求 7-12 任一项所述方法中的所述第一终端和所述第二终端，所述第一终端和所述第二终端执行权利要求 7-12 任一项所述的方法。
15

附图

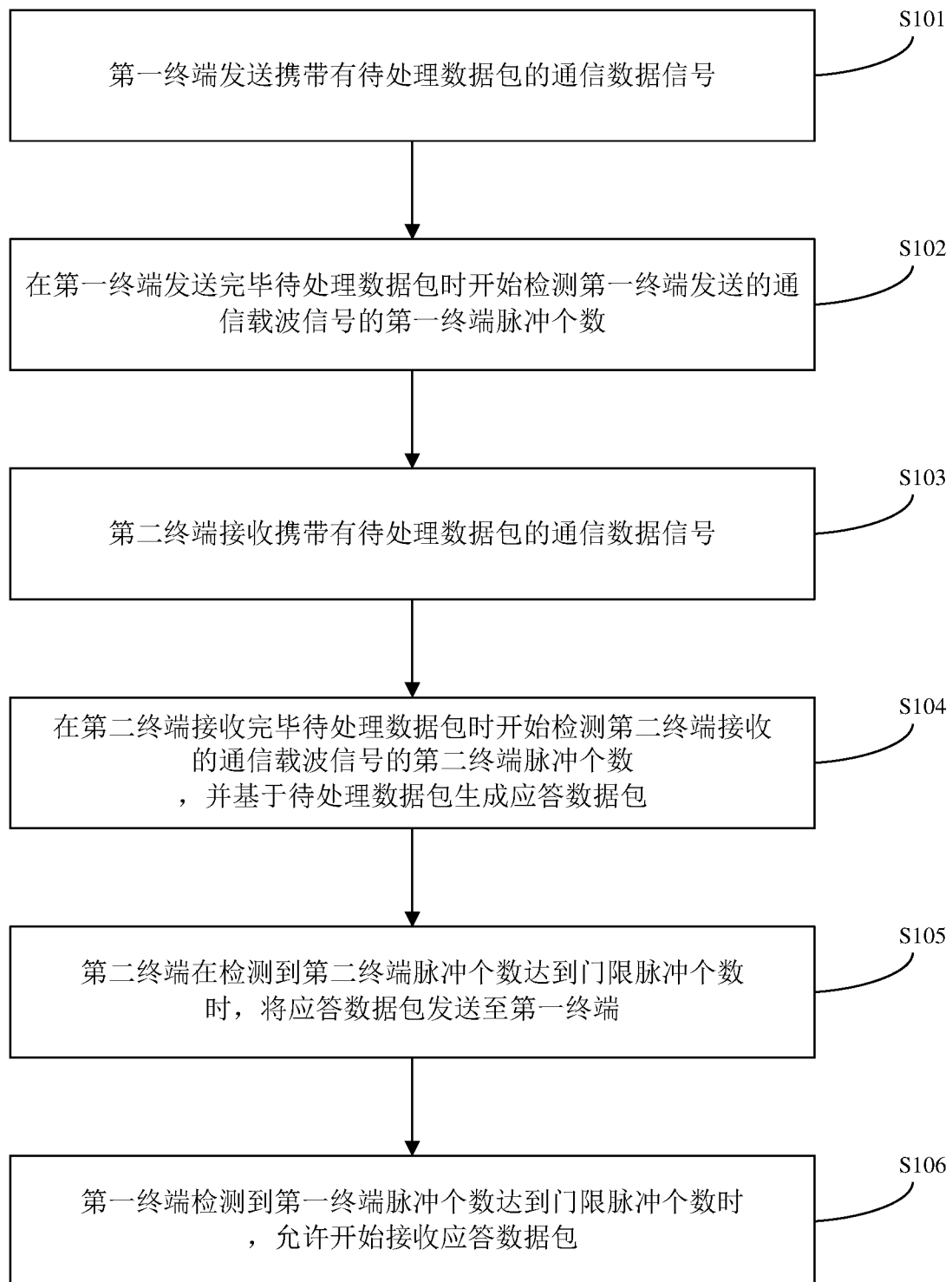


图 1

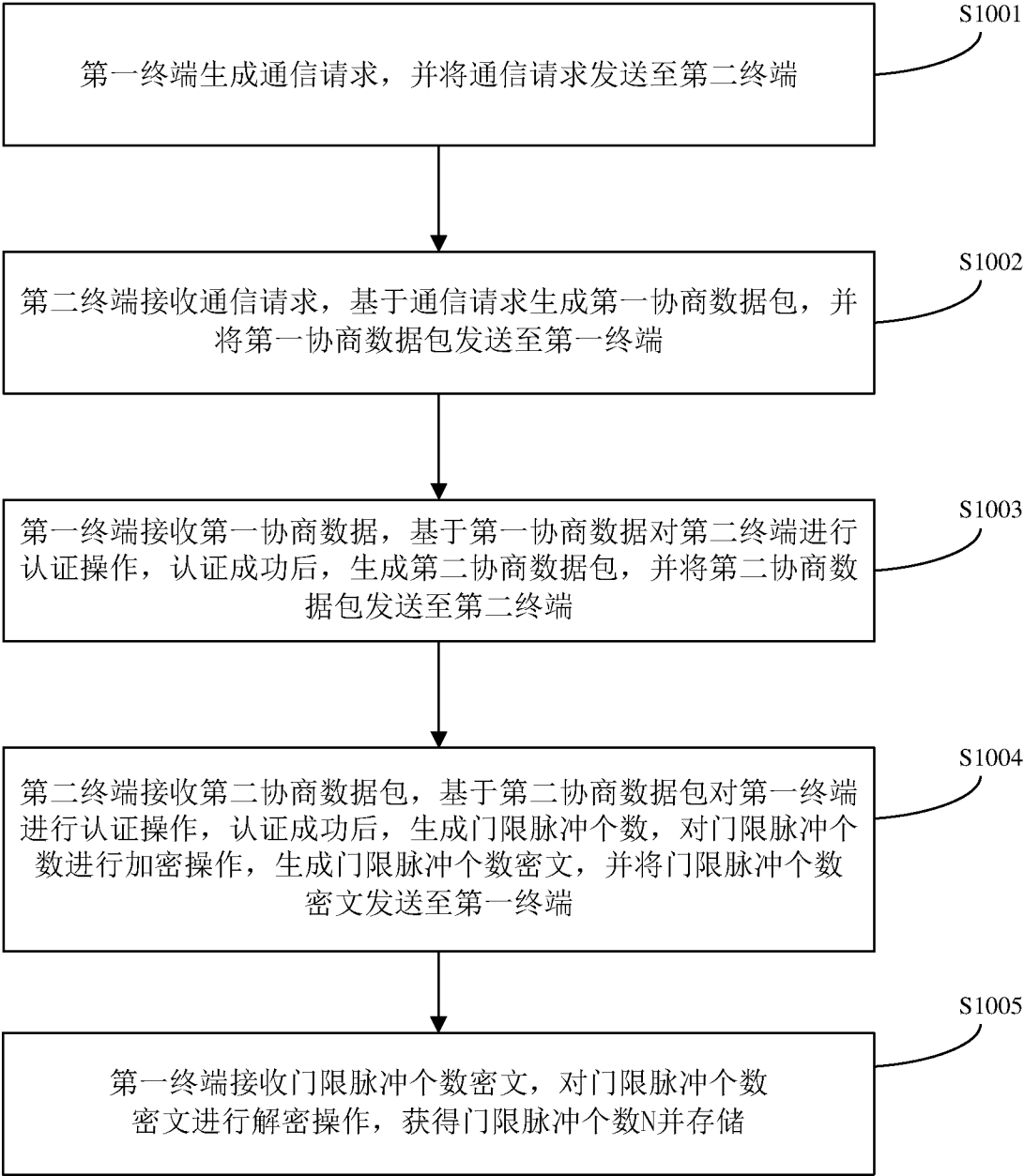


图 2



图 3

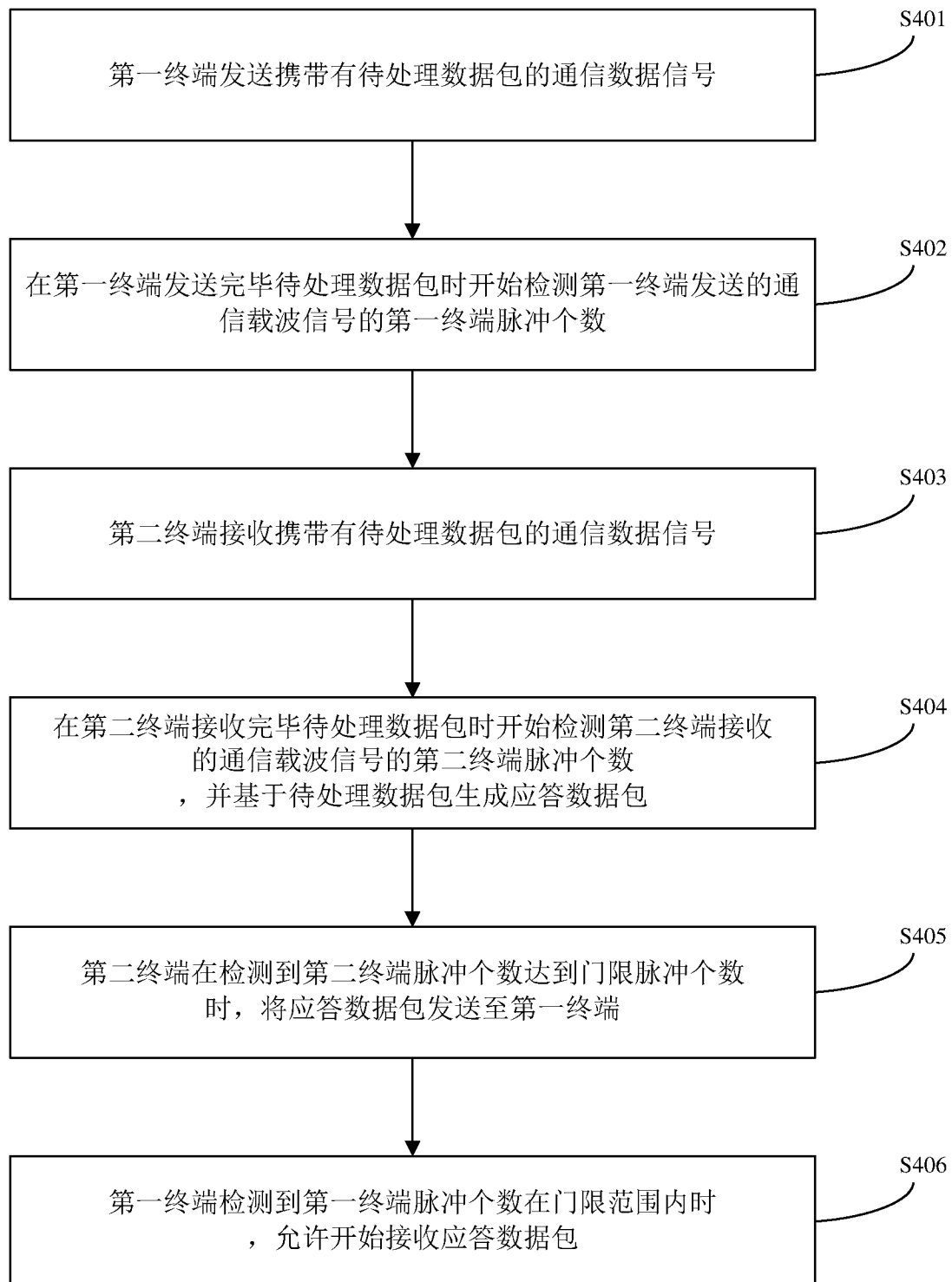


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2017/095990

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i; H04W 12/10 (2009.01) i; H04W 12/02 (2009.01) 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)

H04W 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)

CNPAT, CNKI, WPI, EPODOC, GOOGLE, ISI, IEEE: frame wait, frame delay, near field, near, FWT, FDT, frame wait time, frame delay time, NFC, RFID, IC, phase, difference, tamper, relay, impulse, pulse

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	XIN, Wei, "Research on the Security and Privacy Issues in RFID-Based Supply Chain", CHINA DOCTORAL DISSERTATIONS FULL-TEXT DATABASE, no.10, 15 October 2013 (15.10.2013), chapter six	1-13
A	XIN, Wei et al. "Analysis and Design of Distance-Bounding Protocols for RFID", JOURNAL OF COMPUTER RESEARCH AND DEVELOPMENT, no.11, 30 November 2013 (30.11.2013), the whole document	1-13
A	US 2015264570 A1 (ECOLE POLYTECHNIQUE FEDERALE DE LAUSANNEEPFL), 17 September 2015 (17.09.2015), the whole document	1-13
A	US 2013215788 A1 (QUALCOMM INCORPORATED), 22 August 2013 (22.08.2013), the whole document	1-13
A	CN 103870868 A (SHANGHAI HUAHONG GRACE SEMICONDUCTOR MANUFACTURING CORPORATION), 18 June 2014 (18.06.2014), the whole document	1-13
A	CN 103353597 A (TIANJIN UNIVERSITY), 16 October 2013 (16.10.2013), the whole document	1-13

☐ 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 27 September 2017 (27.09.2017)	Date of mailing of the international search report 27 October 2017 (27.10.2017)
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 CHEN, Gang Telephone No.: (86-10) 62413331

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2017/095990

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US 2015264570 A1	17 September 2015	None	
US 2013215788 A1	22 August 2013	US 2014226550 A1	14 August 2014
		WO 2013126165 A1	29 August 2013
CN 103870868 A	18 June 2014	None	
CN 103353597 A	16 October 2013	None	

国际检索报告

国际申请号

PCT/CN2017/095990

A. 主题的分类

H04L 29/06(2006.01)i; H04W 12/10(2009.01)i; H04W 12/02(2009.01)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)

H04W 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))

CNPAT, CNKI, WPI, EPODOC, GOOGLE, ISI, IEEE: 帧等待, 帧延迟, 帧延时, 近场, 临近, 邻近, 近距离, 相位, 差, 脉冲, 篡改, 中继, FWT, FDT, frame wait time, frame delay time, NFC, RFID, IC, phase, difference, tamper, relay, impulse, pulse

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
A	辛伟. “基于RFID技术的供应链的若干安全与隐私问题研究” 中国博士学位论文全文数据库, 第10期, 2013年 10月 15日 (2013 - 10 - 15), 第六章	1-13
A	辛伟 等. “RFID距离约束协议的分析与设计” 计算机研究与发展, 第11期, 2013年 11月 30日 (2013 - 11 - 30), 全文	1-13
A	US 2015264570 A1 (ECOLE POLYTECHNIQUE FEDERALE DE LAUSANNEEPFL) 2015年 9月 17日 (2015 - 09 - 17) 全文	1-13
A	US 2013215788 A1 (QUALCOMM INCORPORATED) 2013年 8月 22日 (2013 - 08 - 22) 全文	1-13
A	CN 103870868 A (上海华虹宏力半导体制造有限公司) 2014年 6月 18日 (2014 - 06 - 18) 全文	1-13
A	CN 103353597 A (天津大学) 2013年 10月 16日 (2013 - 10 - 16) 全文	1-13

☐ 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 9月 27日

国际检索报告邮寄日期

2017年 10月 27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

陈刚

电话号码 (86-10)62413331

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/095990

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)
US	2015264570	A1	2015年 9月 17日	无			
US	2013215788	A1	2013年 8月 22日	US	2014226550	A1	2014年 8月 14日
				WO	2013126165	A1	2013年 8月 29日
CN	103870868	A	2014年 6月 18日	无			
CN	103353597	A	2013年 10月 16日	无			