(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)

WIPO | PCT

(10) 国际公布号
WO 2018/024250 A1

(51) 国际专利分类号:
G06K 7/00 (2006.01)

(21) 国际申请号: PCT/CN2017/096025

(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:
201610640015.3 2016年8月5日 (05.08.2016) CN
201610639441.5 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,

WO 2018/024250 A1

(54) **Title:** DATA COMMUNICATION METHOD AND DATA COMMUNICATION SYSTEM

(54) 发明名称: 一种数据通讯方法及数据通讯系统

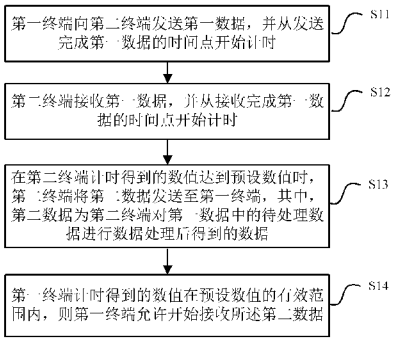

图 3

S11 A FIRST TERMINAL TRANSMITS, TO A SECOND TERMINAL, FIRST DATA, AND UPON COMPLETION OF TRANSMITTING THE FIRST DATA, STARTS MEASURING A TIME VALUE

S12 THE SECOND TERMINAL RECEIVES THE FIRST DATA, AND UPON COMPLETION OF RECEIVING THE FIRST DATA, STARTS MEASURING A TIME VALUE

S13 WHEN THE TIME VALUE OBTAINED BY THE SECOND TERMINAL REACHES A PRECONFIGURED VALUE, THE SECOND TERMINAL PERFORMS DATA PROCESSING ON THE DATA TO BE PROCESSED, AND TRANSMITS, TO A FIRST TERMINAL, SECOND DATA GENERATED AFTER THE DATA PROCESSING

S14 WHEN THE TIME VALUE OBTAINED BY THE FIRST TERMINAL IS IN A VALID RANGE OF A PRECONFIGURED VALUE, THE FIRST TERMINAL IS PERMITTED TO START RECEIVING THE SECOND DATA

(57) **Abstract:** Data communication method and system. The method comprises: a first terminal transmits, to a second terminal, first data, and upon completion of transmitting the first data, starts measuring a time value, wherein the first data comprises data to be processed (S11); the second terminal receives the first data, and upon completion of receiving the first data, starts measuring a time value (S12); when the time value obtained by the second terminal reaches a preconfigured value, the second terminal performs data processing on the data to be processed, and transmits, to a first terminal, second data generated after the data processing (S13); and

[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)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

when the time value obtained by the first terminal is in a valid range of a preconfigured value, the first terminal is permitted to start receiving the second data (S14). By adopting the scheme of the second terminal transmitting data in a fixed time interval and the first terminal receiving the data in another fixed time interval, the first terminal can identify data hijacking at an intermediate node even when the second data is received at the time T2 less than a frame waiting time (FWT).

(57) 摘要: 一种数据通讯方法及系统，该方法包括：第一终端向第二终端发送第一数据，并从发送完成第一数据时开始计时（S11），其中，第一数据至少包括待处理数据；第二终端接收第一数据，并从接收完成第一数据时开始计时（S12）；当第二终端计时得到的数值达到预设数值时，第二终端将对待处理数据进行数据处理后得到的第二数据发送至第一终端（S13）；第一终端计时得到的数值在预设数值的有效范围内，第一终端允许开始接收第二数据（S14）。通过第二终端定时发送第一终端定时接的策略，使得第一终端即使在接收到第二数据的T2<FWT时，仍然可以识别出中间人的劫持。

一种数据通讯方法及数据通讯系统

相关申请的交叉引用

本申请基于申请号为201610640015.3，申请日为2016年8月5日的中国专利申请，以及申请号为201610639441.5，申请日为2016年8月5日的中国专利申请，并要求上述中国专利申请的优先权，上述中国专利申请的全部内容在此引入本申请作为参考。

技术领域

本发明涉及一种电子技术领域，尤其涉及一种数据通讯方法及数据通讯系统。

背景技术

目前现有技术中，采用非接触式的读卡方式的终端都是基于 ISO14443、ISO15693 等协议进行数据传输的，以读卡器与智能卡之间的读卡过程为例，基于上述协议，在读卡器与智能卡的读卡过程中，在读卡器发送了指令数据以后，会有一个帧等待时间（Frame Waiting Time，FWT），表明了读卡器允许等待接收智能卡响应数据的最大时间范围。也就是说在读卡器向智能卡发送了指令以后，读卡器就在等待接收智能卡的响应数据，只要是在帧等待时间 FWT 之内返回的数据，读卡器就会接收。

对于现有的智能卡通讯协议，可能会存在以下问题：对于读卡过程，如图 1 所示，正常情况下商户读卡器将数据发送给用户的智能卡，用户的智能卡接收到数据以后开始响应并处理数据（处理数据时间为 t1），处理结束以后，立即将响应数据发送给商户读卡器，忽略线路传输上的微小时间（数量级很小，便于简化计算），因而，商户读卡器发送数据完成到接收到用户的智能卡反馈的数据所需要的时间 T1=t1。而如果有黑客进行中间人攻击的情况下，如图 2 所示，中间人的智能卡劫持商户读卡器的请求数据，将商户读卡器发来的数据转发至中间人的读卡器，中间人的读卡器可能会篡改请求数据，将篡改后的数据发送至用户的智能卡（从中间人的智能卡劫持商户读卡器的请求数据到中间人的读卡器将篡改后的数据发送至用户的读卡器的时间为 tw1），用户的智能卡接收到篡改后的数据后，处理数据（处理数据时间为 t1），将处理后的数据发送至中间人的读卡器，中间人的读卡器可能会篡改用户的智能卡返回的处理数据，并通过中间人的智能卡将篡改后的数据发送至商户读卡器（从中间人的读卡器接收到用户的智能卡返回的处理数据到通过中间人的智能卡将篡改后的数据发送至商户读卡器的时间为 tw2），那么，商户读卡器从发送完成数据到接收到用户智能卡反馈的数据所需要的时间 T2=t1+tw1+tw2。

根据现有的智能卡通讯协议，只要是 T2<FWT，商户读卡器就会接收中间人的智能卡发来的数据并进行后续的操作（如交易流程），这样就存在中间人劫持而商户读卡器毫不知情的危险，造成商户的经济损失。

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讯方法。

本发明的另一目的在于提供一种数据通讯系统。

为达到上述目的，本发明的技术方案具体是这样实现的：

本发明一方面提供了一种数据通讯方法，包括：第一终端向第二终端发送第一数据，并从发送完成所述第一数据的时间点开始计时，其中，所述第一数据至少包括待处理数据；所述第二终端接收所述第一数据，并从接收完成所述第一数据的时间点开始计时；当所述第二终端计时得到的数值达到预设数值时，所述第二终端将第二数据发送至所述第一终端，其中，所述第二数据为所述第二终端对所述待处理数据进行数据处理后得到的数据；所述第一终端计时得到的数值在所述预设数值的有效范围内，则所述第一终端允许开始接收所述第二数据。

本发明另一方面提供了一种数据通讯系统，包括：第一终端，用于向第二终端发送第一数据，并从发送完成所述第一数据的时间点开始计时，其中，所述第一数据至少包括待处理数据；所述第二终端，用于接收所述第一数据，并从接收完成所述第一数据的时间点开始计时；所述第二终端，还用于当所述第二终端计时得到的数值达到预设数值时，将第二数据发送至所述第一终端，其中，所述第二数据为所述第二终端对所述待处理数据进行数据处理后得到的数据；所述第一终端，还用于若所述第一终端计时得到的数值在所述预设数值的有效范围内，则允许开始接收所述第二数据。

本发明另一方面还提供了一种数据通讯方法，包括：第一终端向第二终端发送第一数据，并从发送完成所述第一数据的时间点开始计时，其中，所述第一数据至少包括待处理数据；所述第二终端接收所述第一数据，并从接收完成所述第一数据的时间点开始计时；在所述第二终端计时得到的数值达到预设数值时，所述第二终端将第二数据发送至所述第一终端，其中，所述第二数据为所述第二终端对所述待处理数据进行数据处理后得到的数据；在所述第一终端计时得到的数值达到所述预设数值时，所述第一终端允许开始接收所述第二数据。

本发明另一方面还提供了一种数据通讯系统，包括：第一终端，用于向第二终端发送第一数据，并从发送完成所述第一数据的时间点开始计时，其中，所述第一数据至少包括待处理数据；所述第二终端，用于接收所述第一数据，并从接收完成所述第一数据的时间点开始计时；所述第二终端，还用于在所述第二终端计时得到的数值达到预设数值时，将第二数据发送至所述第一终端，其中，所述第二数据为所述第二终端对所述待处理数据进行数据处理后得到的数据；所述第一终端，还用于在计时得到的数值达到所述预设数值时，允许开始接收所述第二数据。

由上述本发明提供的技术方案可以看出，本发明提供的数据通讯方法及系统，通过第二终端定时（计时得到的数值达到预设数值 S）发送数据，第一终端定时（计时得到的数

值达到预设数值或在预设数值的有效范围$[S,S+2\Delta S]$内）接收第二终端返回的数据的策略避免现有技术中的问题，由于第一终端只在计时得到的数值达到预设数值或在预设数值的有效范围$[S,S+2\Delta S]$内允许接收第二终端返回的数据，在该预设数值之外或在该预设数值的有效范围之外均不允许接收第二终端返回的数据。由此，如果第一终端在计时得到的数值达到预设数值时，或者如果在该预设数值的有效范围内，允许开始接收且接收到所述第二数据，则说明不存在中间人的劫持，但如果第一终端在计时得到的数值达到预设数值时，或者如果在该预设数值的有效范围内允许开始接收但没有接收到所述第二数据，则说明出现了中间人劫持的情况，使得第一终端即使在接收到第二数据的 T2<FWT 时，仍然可以识别出是否存在中间人劫持的情况，避免用户在毫不知情的情况下造成经济损失。

根据下文结合附图对本发明具体实施例的详细描述，本领域技术人员将会更加明了本发明的上述以及其他目的、优点和特征。

附图说明

后文将参照附图以示例性而非限制性的方式详细描述本发明的一些具体实施例。附图中相同的附图标记标示了相同或类似的部件或部分。本领域技术人员应该理解，这些附图未必是按比例绘制的。附图中：

图 1 为本发明背景技术中在正常情况下商户读卡器发送数据完成到接收到用户的智能卡反馈的数据所需要的时间示意图；

图 2 为本发明背景技术中在发生中间人劫持的情况下商户读卡器发送数据完成到接收到用户的智能卡反馈的数据所需要的时间示意图；

图 3 为本发明实施例 1 提供的数据通讯方法的流程图；

图 4 为本发明实施例 1 提供的一种具体的第一终端与第二终端协商预设数值的流程图；

图 5 为本发明实施例 1 提供的一种具体的第一终端与第二终端协商预设数值的流程图；

图 6 为本发明实施例 2 提供的一种数据通讯系统的结构示意图；

图 7 为本发明实施例 3 提供的数据通讯方法的流程图。

具体实施方式

实施例 1

图 3 为根据本发明实施例 1 的一种数据通讯方法的流程图。参见图 3，该方法至少包括步骤 S11 至步骤 S14。

步骤 S11，第一终端向第二终端发送第一数据，并从发送完成第一数据的时间点开始计时，其中，所述第一数据至少包括待处理数据。

本实施例中，第一终端与第二终端之间的通信方式包括：短距离无线通信方式，具体地，短距离无线通信方式至少包括：NFC（Near Field Communication，近场通讯）、

Wi-Fi(Wireless Fidelity，无线高保真)、UWB（UltraWideband，超宽带）、Zigbee、RFID(Radio Frequency Identification，无线射频识别)、红外传输和蓝牙。因此，第一终端与第二终端之间的通信距离可以短至几厘米长至几百米。基于上述短距离无线通信方式，对应于不同的通信方式，第一终端与第二终端之间通信也会采用对应的通讯协议，以实现两者之间的无线数据传输。其中，作为一种可选的实施方式，第一终端包括读取装置，第二终端包括应答装置，读取装置与应答装置可以为支持非接触式的读卡方式的终端，例如，读取装置可以为 POS 机、ATM 机、身份证阅读器等读卡器类的终端，应答装置可以为智能密钥设备（如工行 U 盾、农行 Key 宝）、智能卡、身份证等终端，采用上述非接触式的读卡方式的终端，如读卡器与智能卡之间、读卡器与身份证之间都可以采用协议 ISO14443 和 ISO15693 进行数据传输，短距离无线通信方式可以包括：ISO14443 和 ISO15693 协议支持的通信方式；此外，读取装置与应答装置也可以为移动终端、PC、掌上电脑、智能设备等支持短距离无线通信方式的终端。

在本步骤中，作为一种可选的实施方式，以第一终端为读卡器，第二终端为智能卡为例，第一数据中的待处理数据可以为读卡请求数据，当然，第一数据中的待处理数据并不限于此，以第一终端与第二终端均为移动终端为例，第一数据中的待处理数据也可以是请求第二终端返回图片的请求数据等等，本实施例并不对第一数据中的待处理数据进行过多限制，只要是第一终端向第二终端发起的请求数据即可。

基于背景技术中提出的问题，本实施例为了能够在 T2<FWT 时，仍然可以识别出中间人的劫持，采用第一终端定时接收第二终端定时发送的策略，所以，在本步骤中，第一终端从发送完成第一数据的时间点开始计时，在计时得到的数值在预设数值的有效范围内时，如果接收到第二终端返回的数据，则说明不存在中间人的劫持，如果没有接收到，则可以识别出存在中间人的劫持。

步骤 S12，第二终端接收第一数据，并从接收完成第一数据的时间点开始计时。

在本实施例中，当第二终端接收到第一数据后，并不会像现有技术那样在对第一数据处理完成后马上将处理后的数据发送至第一终端，而是开始计时，采用第一终端定时接收第二终端定时发送的策略，在计时得到的数值达到预设数值时，第二终端才发送对第一数据中的待处理数据处理后得到的第二数据，即定时发送（参见步骤 S13），使得第一终端在接收到第二数据的 T2<FWT 时，仍然可以识别出是否存在中间人劫持的情况。

步骤 S13，当第二终端计时得到的数值达到预设数值时，第二终端将第二数据发送至第一终端，其中，第二数据为第二终端对第一数据中的待处理数据进行数据处理后得到的数据。

本实施例中，对第二数据并不做限制，第二数据是对第一数据中的待处理数据进行处理后得到的数据。以第二终端为智能卡，第一终端为读卡器为例，第二数据可以为第一终端请求读取的智能卡的数据内容，以第一终端与第二终端均为移动终端为例，第一数据中的待处理数据为请求图片的数据，第二数据即为图片数据。如步骤 S12 中所述，第二终端

在接收完成第一数据的时间点开始计时，本步骤中，在计时得到的数值达到预设数值 S 时，第二终端向第一终端发送第二数据，保证定时发送。

步骤 S14，第一终端计时得到的数值在所述预设数值的有效范围内，则第一终端允许开始接收所述第二数据。

其中，作为一种可选的实施方式，预设数值的有效范围为$[S, S + 2\Delta S]$，其中，S 为预设数值，ΔS由第一终端与第二终端之间采用的通信方式所支持的最大通信距离确定。

本实施例中，正如前面提到的，第一终端与第二终端之间采用的通信方式可以为短距离无线通信，可以包括多种通信方式，而每种通信方式支持的最大通信距离是不同的，例如，NFC 的工作频率为 13.56MHz，支持的通信距离在 20cm 以内，而蓝牙的工作频率为 2.4GHz，支持的通信距离可以达到 20m，WiFi 可以达到 100m。ΔS可以理解为经过第一终端与第二终端之间采用的通信方式所支持的最大通信距离所需的数值，例如，经过该最大通信距离传输第一数据所需的时长等，由于每种通信方式支持的最大通信距离不同，对应的，ΔS的取值也会不同，当然ΔS还可以包括其他含义，具体参见下文的详细描述。

需要说明的是，第一数据是以字节的方式连续发送给第二终端的，第一终端连续发送第一数据的第一字节、第二字节……最后一个字节，第二终端连续接收第一数据的第一字节、第二字节……最后一个字节。由于第一终端与第二终端之间采用短距离通信方式，第一终端开始发送第一数据各个字节的过程中，第二终端已经开始接收第一数据的各个字节，考虑到终端接收单个字节的时长数量级较小，可以忽略不计，因而，第一数据的第一字节在到达第二终端时，第一数据的最后一个字节还没有发送，即第一终端还没有发送完成第一数据。在不考虑路上传输时间的情况下，我们可以认为第一终端发送第一数据与第二终端接收第一数据是同时进行的，即第一终端发送完成第一数据的时刻即为第二终端接收完成第一数据的时刻，在考虑路上传输时间的情况下，第一终端计时得到的数值的最大值可以达到$S + 2\Delta S$，即考虑了第一终端与第二终端之间相互发送的数据在路上传输的时间（根据通信方式支持的最大距离计算得到的最大时长为$2\Delta S$），所以，在步骤 S11 中在第一终端发送完成第一数据的时间点开始计时，在步骤 S12 中，在第二终端接收完成第一数据的时间点开始计时，在不考虑路上传输时间的情况下，没有中间人的劫持，第一终端应该能够在计时得到的数值达到 S 时接收到第二数据，在考虑路上传输时间的情况下，没有中间人的劫持，第一终端应该能够在计时得到的数值大于 S 且小于或等于$S + 2\Delta S$时开始接收第二数据。

基于背景技术中提出的针对现有的智能卡通讯协议存在的问题，本实施例提供了一种数据通讯方法。该数据通讯方法通过第二终端定时（计时得到的数值达到预设数值 S）发送数据，第一终端定时（计时得到的数值在预设数值的有效范围$[S, S + 2\Delta S]$内）接收第二终端返回的数据的策略避免现有技术中的问题，其中，第一终端可以理解为背景技术中的商户读卡器，第二终端可以理解为背景技术中的用户智能卡，由于第一终端只在计时得到的数值在预设数值的有效范围$[S, S + 2\Delta S]$内允许接收第二终端返回的数据，在该预设数值

的有效范围之外均不允许接收第二终端返回的数据。由此，如果在该预设数值的有效范围内，允许开始接收且接收到所述第二数据，则说明不存在中间人的劫持，但如果在该预设数值的有效范围内允许开始接收但没有接收到所述第二数据，则说明出现了中间人劫持的情况。本实施例中，$S + 2\Delta S \leq FWT$，其中，FWT 为第一终端与第二终端采用的通信协议规定的帧等待时间，例如协议 ISO14443 和 ISO15693 规定的帧等待时间 FWT，这样，第一终端（例如读卡器）会在 FWT 的时间内等待智能卡返回数据，同时实施本实施例提供的定时接收的方案，由此，本实施例提供的方法可以在兼容现有协议的同时还可以识别出中间人的劫持。在出现被中间人挟持的情况时，即便 T2<FWT，但是，在不忽略两个终端之间来回传输数据所需的时长$2\Delta S$的情况下，以 S 为预设的时长为例，第二终端计时达到 S 才发送数据，因此，T2= s1+s2+S+$2\Delta S$，其中，T2 为第一终端从发送完成数据到接收到第二终端反馈的数据所需要的时间，s1+s2 为中间人做篡改处理所需的时间（请参考背景技术中 tw1、tw2，tw1 对应 s1，tw2 对应 s2），T2 超过了预设数值的有效范围的最大值 S+$2\Delta S$，所以，第一终端拒绝接收第二终端返回的数据，中断与第二终端的通讯，由此，即便 T2<FWT，第一终端也可以识别出中间人的劫持。需要说明的是，本实施例中 S 与ΔS除了代表时长之外，还可以包括多种形式，此处，为了便于理解，仅以时长为例进行说明，本实施例下文会提到 S 与ΔS包括的多种形式，具体参见下文描述。

在本实施例中，预设数值 S 可以在终端出厂之前预制存储在终端的固定区域中，无需协商，也可以由第一终端与第二终端协商得到，或者，也可以由一方生成发给对方，或者，还可以由第一终端写在协议规定的数据包中，在第一终端向第二终端发送数据时一起发送给第二终端。其中，出厂预制的预设数值虽然无需协商、无需生成，但第一终端与第二终端每次的数据输出均按照该预设数值定时收发，其弊端就是该预设数值不能变化，不够灵活、随机，安全性较低。而后面几种获取预设数值 S 的方式可以随机生成预设数值，相比于出厂预制的预设数值，更灵活，随机，安全性更高。该预设数值 S 对于能否识别出中间人的劫持至关重要，因此，为了防止该预设数值 S 被篡改，本实施例提出了几种获取预设数值 S 的方式，下面便对以下几种获取预设数值 S 的方式进行详细说明。

作为本实施例中一种可选的实施方式，本实施例可以通过以下步骤来实现协商得到预设数值，可以在第一终端向第二终端发送第一数据之前的任何时机进行协商，相比于出厂预制的预设数值，更灵活，随机，安全性更高。具体地，在第一终端从发送完成第一数据的时间点开始计时之前，本实施例提供的方法还包括：

第一终端与第二终端进行双向的身份认证，在所述双向的身份认证通过后，第一终端与第二终端协商得到传输密钥；

第二终端生成该预设数值，并利用所述传输密钥对该预设数值加密，将加密后的预设数值发送至第一终端；第一终端利用所述传输密钥对加密后的预设数值解密得到该预设数值，并保存；或者，第一终端生成该预设数值，并利用所述传输密钥对该预设数值加密，将加密后的预设数值发送至第二终端；第二终端利用所述传输密钥对加密后的预设数值解

密得到该预设数值，并保存。

由此，本实施例可以通过第一终端与第二终端双向的身份认证保证第一终端以及第二终端的合法身份，进一步地协商得到传输密钥，利用该传输密钥对预设数值加解密以保证传输过程的安全性，从而可以防止协商得到的预设数值被非法篡改，保证预设数值的安全性。此外，无论是第一终端还是第二终端，在接收到对方发送的预设数值后进行保存可以在下次数据通信时继续使用该预设数值，通过保存预设数值，两个终端无需再执行协商预设数值的交互流程，大大提高了数据传输效率。

具体地，该可选实施方式中协商得到预设数值的方式可以通过多种方式来实现，本实施例仅举一例，以便于清楚地理解可选实施方式中协商得到预设数值的方式。如图 4 所示，本实施例提供了一种具体的第一终端与第二终端协商预设数值的流程，具体包括以下步骤：

S110，第一终端向第二终端发起认证请求，所述认证请求中携带有随机数 R1 以及第一终端的数字证书。

其中，随机数 R1 为第一终端生成的单次认证数据，可以防止其他非法设备对第一终端的重放攻击。

S111，第二终端接收该认证请求，对第一终端的数字证书进行验证，在验证通过后，利用第二终端的私钥对随机数 R1 进行签名生成签名数据 S1，并生成随机数 R2，利用第一终端的数字证书中的公钥对 R2 加密得到密文 E1。

其中，随机数 R2 为第二终端生成的单次认证数据，可以防止其他非法设备对第二终端的重放攻击。

S112，第二终端将第二终端的数字证书、签名数据 S1 以及密文 E1 发送至第一终端。

S113，第一终端对第二终端的数字证书进行验证，在验证通过后，利用数字证书中的公钥对签名数据 S1 验签，在验签通过后，对密文 E1 解密得到 R2，利用第一终端的私钥对 R2 签名生成签名数据 S2，并生成随机数 R3，利用第二终端的公钥对 R3 加密得到密文 E2，基于 R2R3 生成传输密钥 K。

其中，通过第一终端对第二终端的签名数据 S1 的验签，可以确保第二终端身份的合法性。此外，利用双方各自生成的随机数生成传输密钥，可以保证即使有黑客截获某一方的随机数，但由于没有对方的随机数也无法生成该传输密钥，进而能保证传输密钥不会被轻易获取。

S114，第一终端将签名数据 S2 和密文 E2 发送至第二终端。

S115，第二终端利用第一终端的数字证书中的公钥对签名数据 S2 验签，在验签通过后，对密文 E2 解密得到 R3，基于 R2R3 生成传输密钥 K。

其中，通过第二终端对第一终端的签名数据 S2 的验签，可以确保第一终端身份的合法性。

S116，第一终端生成预设数值 S，利用传输密钥 K 加密得到密文 E3。

S117，第一终端将 E3 发送至第二终端。

S118，第二终端接收密文 E3，并利用传输密钥 K 对 E3 解密得到预设数值 S，并保存预设数值 S。

在该可选实施方式中，从步骤 S110~步骤 S115 完成了第一终端与第二终端的双向认证以及协商传输密钥，在步骤 S116~S118 中，第一终端与第二终端执行的操作可以互换，即，可以由第二终端生成预设数值 S，利用 K 加密 S 得到密文 E3，发送至第一终端，第一终端利用传输密钥 K 解密得到预设数值 S，并保存。

作为本实施例中另一种可选的实施方式，本实施例可以通过以下步骤来实现由一方生成发给对方得到预设数值的方式，可以在第一终端向第二终端发送第一数据之前的任何时机进行协商，相比于出厂预制的预设数值，更灵活，随机，安全性更高。具体地，在第一终端从发送完成第一数据的时间点开始计时之前，本实施例提供的方法还包括：

第一终端与第二终端进行双向的身份认证；

在所述双向的身份认证通过后，第二终端生成该预设数值，并利用第一终端的公钥对该预设数值加密，将加密后的预设数值发送至第一终端；第一终端利用其私钥对加密后的预设数值解密得到该预设数值，并保存；或者，在所述双向的身份认证通过后，第一终端生成该预设数值，并利用第二终端的公钥对该预设数值加密，将加密后的预设数值发送至第二终端；第二终端利用其私钥对加密后的预设数值解密得到该预设数值，并保存。

由此，本实施例可以通过第一终端与第二终端双向的身份认证保证第一终端以及第二终端的合法身份，进一步利用公私钥实现对预设数值加解密以保证传输过程的安全性，从而可以防止一方生成的预设数值被非法篡改，保证预设数值的安全性。相比于上面的可选实施方式，该可选实施方式利用第一终端和第二终端本身的公私钥对实现对预设数值的加解密，无需再生成传输密钥，减少了交互步骤，缩短了获得预设数值的时间，提高了效率。此外，无论是第一终端还是第二终端，在接收到对方发送的预设数值后进行保存可以在下次数据通信时继续使用该预设数值，通过保存预设数值，两个终端无需再执行协商预设数值的交互流程，大大提高了数据传输效率。

具体地，该可选实施方式中得到预设数值的方式可以通过多种方式来实现，本实施例仅举一例，以便于清楚地理解可选实施方式中得到预设数值的方式。如图 5 所示，本实施例提供了一种具体的第一终端与第二终端协商预设数值的流程，具体包括以下步骤：

S120，第一终端向第二终端发起认证请求，所述认证请求中携带有随机数 R1；

其中，随机数 R1 为第一终端生成的单次认证数据，可以防止其他非法设备对第一终端的重放攻击。

S121，第二终端接收该认证请求，并利用其私钥对随机数 R1 进行签名生成签名数据 S1，并生成随机数 R2；

其中，随机数 R2 为第二终端生成的单次认证数据，可以防止其他非法设备对第二终端的重放攻击。

S122，第二终端将第二终端的数字证书、签名数据 S1 以及随机数 R2 发送至第一终端；

S123，第一终端对第二终端的数字证书进行验证，在验证通过后，利用数字证书中的公钥对签名数据 S1 验签，在验签通过后，利用第一终端的私钥对 R2 签名生成签名数据 S2；

其中，通过第一终端对第二终端的签名数据 S1 的验签，可以确保第二终端身份的合法性。

S124，第一终端将其数字证书和签名数据 S2 发送至第二终端；

S125，第二终端对第一终端的数字证书进行验证，在验证通过后，利用数字证书中的公钥对签名数据 S2 验签；

其中，通过第二终端对第一终端的签名数据 S2 的验签，可以确保第一终端身份的合法性。

S126，在验签通过后，第二终端随机生成预设数值 S，利用第一终端的公钥对预设数值 S 加密生成密文 E；

S127，第二终端将 E 发送至第一终端；

S128，第一终端接收密文 E，并利用其私钥对 E 解密得到预设数值 S，并保存预设数值 S。

在该可选实施方式中，从步骤 S120~步骤 S125 实现了第一终端与第二终端之间的双向认证，并在双向的身份认证通过后，第二终端生成预设数值，在步骤 S126~S128 中，第一终端与第二终端执行的操作可以互换，即，可以由第一终端生成预设数值 S，利用第二终端的公钥对预设数值 S 加密得到密文 E，发送至第二终端，第二终端利用其私钥对 E 解密得到预设数值 S，并保存。与图 4 所示的获取预设数值的方式相比，该可选实施方式无需协商传输密钥，而是直接利用第一终端与第二终端本身的公私钥进行加解密，减少了协商传输密钥的交互流程，可以提高获得预设数值的效率。

作为本实施例中第三种可选的实施方式，本实施例可以通过以下步骤来实现由第一终端将预设数值写入协议规定的数据包中，在第一终端向第二终端发送数据时一起发送给第二终端来实现双方得到该预设数值，具体地，在步骤 S11 中第一终端向第二终端发送第一数据之前，本实施例提供的方法还包括：第一终端生成预设数值；在第一终端发送给第二终端的第一数据中至少还包括：该预设数值以及基于该预设数值计算得到的防篡改校验值；在步骤 S12 中，第二终端接收第一数据之后，本实施例提供的方法还包括：第二终端从第一数据中获取该预设数值以及防篡改校验值，并对防篡改校验值进行校验，在校验通过后，保存该预设数值。

在该可选实施方式中，第一终端可以随机生成一个预设数值，根据协议规定的数据包的格式，将该预设数值和防篡改校验值写入预定字段中，或者，也可以增加新的字段，将该预设数值和防篡改校验值写入新增的字段中，在第一终端向第二终端发送第一数据时，携带在第一数据中的数据包中发送至第二终端。该防窜改校验值是基于预设数值计算得到的，例如，该防窜改校验值可以为基于该预设数值计算得到的签名数据，即对预设数值计算生成摘要，并利用第一终端的私钥对摘要加密生成签名数据，第二终端在对防窜改校验

值进行校验就可以利用第一终端的公钥对该签名数据进行验签，如果验签通过，则校验通过，说明预设数值没有被篡改。又例如，该防窜改校验值可以为基于预设数值采用 MAC 算法计算得到的 MAC 值，第二终端在对防窜改校验值进行校验时也可以采用相同的 MAC 算法计算得到一个 MAC 值，比较两个 MAC 值是否一致，如果一致，则校验通过，说明预设数值没有被篡改。

需要说明的是，第二终端在接收完成第一数据后，开始计时，并从第一数据中获取预设数值，如果对防篡改校验值校验通过，则所述第二终端在计时得到的数值达到预设数值后发送第二数据至第一终端，后续如果第一终端在预设数值的有效范围内接收不到第二终端返回的第二数据，则说明出现了中间人劫持；如果对防窜改校验值的校验不通过，第二终端会停止计时，此时说明已经有可能出现了中间人劫持数据的情况。由此，在该可选实施方式中，通过防窜改校验值也可以实现中间人劫持的识别，而且，一旦预设数值被篡改，校验就不能通过，进而可以保证预设数值不会被非法篡改，保证预设数值的安全。

此外，在本实施例中，作为一种可选的实施方式，预设数值可以至少包括：预设的时长、预设的周期个数、预设的脉冲个数或者预设的相位差，因此，本实施例中，第一终端和第二终端也相应地有不同的计时统计方式，以及判断计时得到的数值是否达到预设数值或在预设数值的有效范围内的方式，下面分别针对各种预设数值进行详细的说明。

作为一种本实施例可选的实施方式，预设数值可以包括：预设的时长，其中，该预设的时长大于第二终端对接收到的第一数据中的待处理数据进行数据处理的时长（由于第二终端需要在处理数据之后达到计时得到的数值才发送第二数据），此外，可选地，$S + 2\Delta S \leq FWT$；ΔS为在第一终端与第二终端之间的距离为两者采用的通信方式所支持的最大通信距离时，第一终端传输数据至第二终端所需的时长，在步骤 S14 中，第一终端计时得到的数值在预设数值的有效范围内，包括：第一终端从发送完成第一数据之后计时得到的时长在$[S, S + 2\Delta S]$范围内；在步骤 S13 中，第二终端计时得到的数值达到预设数值，包括：第二终端从接收完成第一数据之后计时得到的时长达到预设的时长。

在该种可选实施方式中，第一终端与第二终端中均具有计时器，支持精确计时功能，可以通过计时器计时得到的时长判断是否达到预设时长或是否在预设时长的有效范围内。例如，第二终端可以为具有晶振的智能卡，该具有晶振的智能卡可以通过其内部时钟计时的时长的方式来统计计时，其计时精确度由智能卡的时钟精确度决定。例如，$S = 5 \times 10^{-3}$s，以蓝牙为例，支持的最大传输距离 20m 的传输时长ΔS为60×10^{-9}s，则第二终端在计时达到5×10^{-3}s时发送第二数据，第一终端只有在$[5 \times 10^{-3}\text{s}, (5 \times 10^{-3} + 1.2 \times 10^{-7})\text{s}]$才允许开始接收第二数据，只有在该预设数值的有效范围内接收到第二数据才说明没有出现中间人的劫持的情况，由此，可以识别出中间人的劫持。虽然，该可选实施方式仅以蓝牙通信方式进行了举例说明，但其他短距离通信方式均属于本发明保护的范围。

对于无源、无晶振的终端（如智能卡）来说，该终端没有计时功能，而在本实施例中，由于在第一终端与第二终端通信的整个过程中，第一终端始终产生载波信号，因此，本实

施例中提出了有别与时钟计时的计时统计方式，本实施例还可以通过计算载波信号的周期个数、脉冲个数以及相位差来统计计时得到的数值，预设数值具体可以包括：预设的载波信号的周期个数、预设的载波信号的脉冲个数以及预设的载波信号的相位差，ΔS具体可以指示载波信号经过第一终端与第二终端之间采用的通信方式所支持的最大通信距离所产生的周期个数、脉冲个数，以及相位变化值，其中，无论采用上述哪一种计时统计方式，$S+2\Delta S$的和对应的时长均大于第二终端对接收到的第一数据中的待处理数据进行数据处理的时长，此外，可选地，$S+2\Delta S$的和对应的时长均可以小于或等于 FWT。作为一种可选的实施方式，预设数值可以包括：预设的周期个数；ΔS为载波信号经过第一终端与第二终端之间采用的通信方式所支持的最大通信距离所产生的周期个数；在步骤 S14 中，第一终端计时得到的数值在预设数值的有效范围内，包括：第一终端从发送完成第一数据之后持续向第二终端发送的载波信号的周期个数在所述$[S,S+2\Delta S]$范围内；步骤 S13 中，第二终端计时得到的数值达到预设数值，包括：第二终端从接收完成第一数据之后持续接收到的载波信号的周期个数达到预设的周期个数。

在本实施例中，第一终端始终在产生载波信号，在第一终端需要发送数据时，例如，第一终端发送第一数据是将第一数据调制在载波信号上发送至第二终端的，在第一终端不需要发送数据时，第一终端发送该载波信号至第二终端，该载波信号上没有携带数据。该可选实施方式中，第一终端与第二终端均具有计数器，可以计算上述情况下载波的周期个数，该可选实施方式提供了一种可选的统计计时得到的数值的方式，第一终端与第二终端无需使用时钟计时，也可以达到精确计时的目的，举例来说，以支持 NFC 通信方式的终端为例，第一终端与第二终端的工作频率为 13.56MHZ，在第一终端与第二终端通信过程中，第一终端（例如读卡器）始终产生 13.56MHz 的载波，载波的时间周期 T 是固定的，T=1/13.56MHz，约等于 74ns，以周期来统计计时得到的数值，单位可以精确到 ns，由此可以达到精确统计的效果，而且，该可选实施方式可以适用于无源无晶振的智能卡。虽然，该可选实施方式仅以 NFC 通信方式进行了举例说明，但其他短距离通信方式均属于本发明保护的范围。

此外，作为另一种本实施例可选的实施方式，预设数值可以包括：预设的脉冲个数；ΔS为载波信号经过第一终端与第二终端之间采用的通信方式所支持的最大通信距离所产生的脉冲个数；在步骤 S14 中，第一终端计时得到的数值在预设数值的有效范围内，包括：第一终端从发送完成第一数据之后持续向第二终端发送的载波信号的脉冲个数在$[S,S+2\Delta S]$范围内；在步骤 S13 中，第二终端计时得到的数值达到预设数值，包括：第二终端从接收完成第一数据之后持续接收到的载波信号的脉冲个数达到预设的脉冲个数。

统计载波信号的脉冲个数即统计载波信号的峰值的个数，相比于上述统计载波信号的周期个数的方式，统计脉冲个数可以达到进一步精确统计的效果，而且，该可选实施方式可以适用于无源无晶振的智能卡。

此外，作为另一种本实施例可选的实施方式，预设数值可以包括：预设的相位差；ΔS

为载波信号经过第一终端与第二终端之间采用的通信方式所支持的最大通信距离所产生的相位变化值；在步骤 S14 中，第一终端计时得到的数值在预设数值的有效范围内，包括：载波信号在第一相位与第二相位的相位差在$[S, S+2\Delta S]$范围内，其中，第一相位为载波信号在第一终端发送完成第一数据的时间点的相位，第二相位为载波信号在第一终端允许开始接收第二数据的时间点的相位；在步骤 S13 中，第二终端计时得到的数值达到预设数值，包括：载波信号在第三相位与第四相位的相位差达到预设的相位差，其中，第三相位为载波信号在第二终端在接收完成第一数据的时间点的相位，第四相位为载波信号在第二终端开始发送所述第二数据的时间点的相位。

例如，第一终端与第二终端可以采用之前提到的获得预设数值的方式，协商或一方生成预设的相位差$S=(1/2+40)\pi$，在以第一终端为读卡器，第二终端为智能卡为例，读卡器在发送完成第一数据后以及智能卡在接收完成该第一数据后，两者之间的通信波形就是标准的正弦波载波，记录此刻的相位为 0（即第一相位与第三相位为 0），在载波相位差（即第三相位与第四相位的相位差）达到$(1/2+40)\pi$时，智能卡发送第二数据，此时，读卡器可以通过计时得到的相位差在预设数值的有效范围内允许开始接收且接收到第二数据，来确认没有中间人的劫持。以 NFC 为例，假设携带有第一数据的载波信号经过 NFC 支持的最大传输距离 20cm 所产生的相位变化值$\Delta S=\frac{1}{4}\pi$，则第一终端只有在$[(1/2+40)\pi, 41\pi]$才允许开始接收第二数据，只有在该预设数值的有效范围内接收到第二数据才说明没有出现中间人的劫持的情况，由此，可以识别出中间人的劫持。

在该可选实施方式中，以支持 NFC 通信方式的终端为例，第一终端与第二终端的工作频率为 13.56MHz，在第一终端与第二终端通信过程中，第一终端（例如读卡器）始终产生 13.56MHz 的载波，载波的时间周期是固定的，T=1/13.56MHz，约等于 74ns，相位是可以将一个周期在 2π的角度来划分，以相位来统计计时，单位可以精确到 74/2π ns，相比于上述统计载波信号的周期个数以及脉冲个数的方式，统计相位差可以达到进一步精确统计的效果，而且，该可选实施方式可以适用于无源无晶振的智能卡。虽然，该可选实施方式仅以 NFC 通信方式进行了举例说明，但其他短距离通信方式均属于本发明保护的范围。

通过本发明实施例提供的数据通讯方法，通过第一终端定时接收第二终端定时发送的策略，使得第一终端即使在接收到第二数据的T2<FWT时，仍然可以识别出是否存在中间人劫持的情况，避免用户在毫不知情的情况下造成经济损失。

实施例 2

基于同一发明构思，本发明实施例还提供一种数据通讯系统。如图 6 所示，该数据通讯系统包括：第一终端和第二终端，第一终端和第二终端执行如实施例 1 中的数据通讯方法。其中：

第一终端，用于向第二终端发送第一数据，并从发送完成第一数据的时间点开始计时，其中，第一数据至少包括待处理数据；第二终端，用于接收第一数据，并从接收完成第一数据的时间点开始计时；第二终端，还用于当第二终端计时得到的数值达到预设数值时，将第二数据发送至第一终端，其中，第二数据为第二终端对待处理数据进行数据处理后得到的数据；第一终端，还用于若第一终端计时得到的数值在预设数值的有效范围内，则允许开始接收第二数据。

作为一种可选的实施方式，预设数值的有效范围为$[S, S+2\Delta S]$，其中，S 为预设数值，ΔS由第一终端与第二终端之间采用的通信方式所支持的最大通信距离确定，其中，$S+2\Delta S$对应的时长小于或等于第一终端与第二终端采用的通信协议规定的帧等待时间 FWT。

作为一种可选的实施方式，第一终端与第二终端之间的通信方式包括：短距离无线通信方式。

作为一种可选的实施方式，第一终端，还用于在第一终端从发送完成第一数据的时间点开始计时之前，与第二终端进行双向的身份认证，在双向的身份认证通过后，与第二终端协商得到传输密钥；

第二终端，还用于生成预设数值，并利用传输密钥对预设数值加密，将加密后的预设数值发送至第一终端；第一终端，还用于利用传输密钥对加密后的预设数值解密得到预设数值，并保存；或者，

第一终端，还用于生成预设数值，并利用传输密钥对预设数值加密，将加密后的预设数值发送至第二终端；第二终端，还用于利用传输密钥对加密后的预设数值解密得到预设数值，并保存。

作为一种可选的实施方式，第一终端，还用于在第一终端从发送完成第一数据的时间点开始计时之前，与第二终端进行双向的身份认证；

第二终端，还用于在双向的身份认证通过后，生成预设数值，并利用第一终端的公钥对预设数值加密，将加密后的预设数值发送至第一终端；第一终端，还用于利用第一终端的私钥对加密后的预设数值解密得到预设数值，并保存；

或者，

第一终端，还用于在双向的身份认证通过后，生成预设数值，并利用第二终端的公钥对预设数值加密，将加密后的预设数值发送至第二终端；第二终端，还用于利用第二终端的私钥对加密后的预设数值解密得到预设数值，并保存。

作为一种可选的实施方式，第一终端，还用于在第一终端向第二终端发送第一数据之前，生成预设数值；第一数据至少还包括：预设数值以及基于预设数值计算得到的防篡改校验值；第二终端，还用于在接收第一数据之后，还从第一数据中获取预设数值以及防篡改校验值，并对防篡改校验值进行校验，在校验通过后，保存预设数值。

作为一种可选的实施方式，预设数值包括：预设的时长；ΔS为在第一终端与第二终端之间的距离为两者采用的通信方式所支持的最大通信距离时，第一终端传输数据至第二终

端所需的时长；第一终端计时得到的数值在预设数值的有效范围内，包括：第一终端从发送完成第一数据之后计时得到的时长在$[S, S+2\Delta S]$范围内；第二终端计时得到的数值达到预设数值，包括：第二终端从接收完成第一数据之后计时得到的时长达到预设的时长；或者，

预设数值包括：预设的周期个数；第一终端，还用于在第一终端与第二终端通信的整个过程中，始终产生载波信号；ΔS为载波信号经过第一终端与第二终端之间采用的通信方式所支持的最大通信距离所产生的周期个数；其中：第一终端计时得到的数值在预设数值的有效范围内，包括：第一终端从发送完成第一数据之后持续向第二终端发送的载波信号的周期个数在$[S, S+2\Delta S]$范围内；第二终端计时得到的数值达到预设数值，包括：第二终端从接收完成第一数据之后持续接收到的载波信号的周期个数达到预设的周期个数；或者，

预设数值包括：预设的脉冲个数；第一终端，还用于在第一终端与第二终端通信的整个过程中，始终产生载波信号；ΔS为载波信号经过第一终端与第二终端之间采用的通信方式所支持的最大通信距离所产生的脉冲个数；其中：第一终端计时得到的数值在预设数值的有效范围内，包括：第一终端从发送完成第一数据之后持续向第二终端发送的载波信号的脉冲个数在$[S, S+2\Delta S]$范围内；第二终端计时得到的数值达到预设数值，包括：第二终端从接收完成第一数据之后持续接收到的载波信号的脉冲个数达到预设的脉冲个数；或者，

预设数值包括：预设的相位差；第一终端，还用于在第一终端与第二终端通信的整个过程中，始终产生载波信号；ΔS为载波信号经过第一终端与第二终端之间采用的通信方式所支持的最大通信距离所产生的相位变化值；其中：第一终端计时得到的数值在预设数值的有效范围内，包括：载波信号在第一相位与第二相位的相位差在$[S, S+2\Delta S]$范围内，其中，第一相位为载波信号在第一终端发送完成第一数据的时间点的相位，第二相位为载波信号在第一终端允许开始接收第二数据的时间点的相位；第二终端计时得到的数值达到预设数值，包括：载波信号在第三相位与第四相位的相位差达到预设的相位差，其中，第三相位为载波信号在第二终端在接收完成第一数据的时间点的相位，第四相位为载波信号在第二终端开始发送第二数据的时间点的相位。

通过本发明实施例提供的数据通讯系统，通过第一终端定时接收第二终端定时发送的策略，使得第一终端即使在接收到第二数据的T2<FWT时，仍然可以识别出是否存在中间人劫持的情况，避免用户在毫不知情的情况下造成经济损失。

实施例3

图 7 为根据本发明实施例 3 的一种数据通讯方法的流程图。参见图 7，该方法至少包括步骤 S31 至步骤 S34。

步骤 S31，第一终端向第二终端发送第一数据，并从发送完成第一数据的时间点开始计时，其中，所述第一数据至少包括待处理数据。

本实施例中，第一终端与第二终端之间的通信方式包括：短距离无线通信方式，具体

地，可参见实施例 1 中步骤 S11 中的相应描述。

在本步骤中，作为一种可选的实施方式，以第一终端为读卡器，第二终端为智能卡为例，第一数据中的待处理数据可以为读卡请求数据，当然，第一数据中的待处理数据并不限于此，以第一终端与第二终端均为移动终端为例，第一数据中的待处理数据也可以是请求第二终端返回图片的请求数据等等，本实施例并不对第一数据中的待处理数据进行过多限制，只要是第一终端向第二终端发起的请求数据即可。

基于背景技术中提出的问题，本实施例为了能够在 T2<FWT 时，仍然可以识别出中间人的劫持，采用第一终端定时接收第二终端定时发送的策略，所以，在本步骤中，第一终端从发送完成第一数据的时间点开始计时，在所述第一终端计时得到的数值达到所述预设数值时，如果接收到第二终端返回的数据，则说明不存在中间人的劫持，如果没有接收到，则可以识别出存在中间人的劫持。

步骤 S32，第二终端接收第一数据，并从接收完成第一数据的时间点开始计时。

在本实施例中，当第二终端接收到第一数据后，并不会像现有技术那样在对第一数据处理完成后马上将处理后的数据发送至第一终端，而是开始计时，采用第一终端定时接收第二终端定时发送的策略，在计时得到的数值达到预设数值时，第二终端才发送对第一数据中的待处理数据处理后得到的第二数据，即定时发送（参见步骤 S33），使得第一终端在接收到第二数据的 T2<FWT 时，仍然可以识别出是否存在中间人劫持的情况。

步骤 S33，在第二终端计时得到的数值达到预设数值时，第二终端将第二数据发送至第一终端，其中，第二数据为第二终端对第一数据中的待处理数据进行数据处理后得到的数据。

本实施例中，对第二数据并不做限制，具体地，可参见实施例 1 中步骤 S13 中的相应描述。

步骤 S34，在第一终端计时得到的数值达到预设数值时，则第一终端允许开始接收所述第二数据。

本实施例中，正如前面提到的，第一终端与第二终端之间采用的通信方式可以为短距离无线通信，可以包括多种通信方式，而每种通信方式支持的最大通信距离是不同的，例如，NFC 的工作频率为 13.56MHz，支持的通信距离在 20cm 以内，而蓝牙的工作频率为 2.4GHz，支持的通信距离可以达到 20m，WiFi 可以达到 100m。基于短距离无线通信支持的最大通信距离均在几百米以内，数据在两个终端之间的传输时间为 ns 级，而预设数值至少要大于第二终端对待处理数据进行数据处理的时间（ms 级），因此，由于数据在两个终端之间的路上传输时间相比于预设数值非常微小，在本实施例中，数据的传输时间可以忽略不计。

需要说明的是，第一数据是以字节的方式连续发送给第二终端的，第一终端连续发送第一数据的第一字节、第二字节……最后一个字节，第二终端连续接收第一数据的第一字节、第二字节……最后一个字节。由于第一终端与第二终端之间采用短距离通信方式，第

一终端开始发送第一数据各个字节的过程中，第二终端已经开始接收第一数据的各个字节，考虑到终端接收单个字节的时长数量级较小，可以忽略不计，因而，第一数据的第一字节在到达第二终端时，第一数据的最后一个字节还没有发送，即第一终端还没有发送完成第一数据。在不考虑路上传输时间的情况下，我们可以认为第一终端发送第一数据与第二终端接收第一数据是同时进行的，即第一终端发送完成第一数据的时刻即为第二终端接收完成第一数据的时刻，所以，在步骤 S31 中在第一终端发送完成第一数据的时间点开始计时，在步骤 S32 中，在第二终端接收完成第一数据的时间点开始计时，在不考虑路上传输时间的情况下，没有中间人的劫持，第一终端应该能够在计时得到的数值达到预设数值时接收到第二数据。

基于背景技术中提出的针对现有的智能卡通讯协议存在的问题，本实施例提供了一种数据通讯方法。该数据通讯方法通过第二终端定时（计时得到的数值达到预设数值）发送数据，第一终端定时（计时得到的数值达到预设数值）接收第二终端返回的数据的策略避免现有技术中的问题，其中，第一终端可以理解为背景技术中的商户读卡器，第二终端可以理解为背景技术中的用户智能卡，由于第一终端只在计时得到的数值达到预设数值时允许接收第二终端返回的数据，在该预设数值之外的任何数值（例如未达到或超过该预设数值）均不允许接收第二终端返回的数据。由此，如果第一终端在计时得到的数值达到预设数值时，允许开始接收且接收到所述第二数据，则说明不存在中间人的劫持，但如果在第一终端在计时得到的数值达到预设数值时允许开始接收但没有接收到所述第二数据，则说明出现了中间人劫持的情况。本实施例中预设数值 S 对应的时长小于或等于第一终端与第二终端采用的通信协议规定的帧等待时间 FWT，例如协议 ISO14443 和 ISO15693 规定的帧等待时间 FWT，这样，第一终端（例如读卡器）会在 FWT 的时间内等待智能卡返回数据，同时实施本实施例提供的定时接收的方案，由此，本实施例提供的方法可以在兼容现有协议的同时还可以识别出中间人的劫持。在出现被中间人挟持的情况时，即便 T2<FWT，但是，在忽略两个终端之间来回传输数据所需的时长的情况下，以预设数值 S 为预设的时长为例，第二终端计时达到 S 才发送数据，因此，T2= s1+s2+S，其中，T2 为第一终端从发送完成数据到接收到第二终端反馈的数据所需要的时间，s1+s2 为中间人做篡改处理所需的时间（请参考背景技术中 tw1、tw2，tw1 对应 s1，tw2 对应 s2），T2 超过了预设数值 S，所以，第一终端拒绝接收第二终端返回的数据，中断与第二终端的通讯，由此，即便 T2<FWT，第一终端也可以识别出中间人的劫持。需要说明的是，本实施例中预设数值 S 除了代表时长之外，还可以包括多种形式，此处，为了便于理解，仅以时长为例进行说明，本实施例下文会提到预设数值包括的多种形式，具体参见下文描述。

在本实施例中，预设数值可以在终端出厂之前预制存储在终端的固定区域中，无需协商，也可以由第一终端与第二终端协商得到，或者，也可以由一方生成发给对方，或者，还可以由第一终端写在协议规定的数据包中，在第一终端向第二终端发送数据时一起发送给第二终端。该预设数值对于能否识别出中间人的劫持至关重要，因此，为了防止该预设

数值被篡改，本实施例提出了几种获取预设数值的方式，具体可以参见实施例 1 中对于几种获取预设数值的方式的详细说明。

此外，在本实施例中，作为一种可选的实施方式，预设数值可以至少包括：预设的时长、预设的周期个数、预设的脉冲个数或者预设的相位差，因此，本实施例中，第一终端和第二终端也相应地有不同的计时统计方式，以及判断计时得到的数值是否达到预设数值的方式，下面分别针对各种预设数值进行详细的说明。

作为一种本实施例可选的实施方式，预设数值可以包括：预设的时长，其中，该预设的时长大于第二终端对接收到的第一数据中的待处理数据进行数据处理的时长（由于第二终端需要在处理数据之后达到计时得到的数值才发送第二数据），此外，可选地，预设的时长可以小于或等于 FWT；在步骤 S34 中，第一终端计时得到的数值达到预设数值，包括：第一终端从发送完成第一数据之后计时得到的时长达到预设的时长；在步骤 S33 中，第二终端计时得到的数值达到预设数值，包括：第二终端从接收完成第一数据之后计时得到的时长达到预设的时长。

在该种可选实施方式中，第一终端与第二终端中均具有计时器，支持精确计时功能，可以通过计时器计时得到的时长判断是否达到预设时长或是否在预设时长范围内。例如，第二终端可以为具有晶振的智能卡，该具有晶振的智能卡可以通过其内部时钟计时的时长的方式来统计计时，其计时精确度由智能卡的时钟精确度决定。例如，$S = 5 \times 10^{-3}$s，以蓝牙为例，第二终端在计时达到5×10^{-3}s时发送第二数据，第一终端只有在计时达到5×10^{-3}s时才允许开始接收第二数据，只有在计时达到5×10^{-3}s时接收到第二数据才说明没有出现中间人的劫持的情况，由此，可以识别出中间人的劫持。虽然，该可选实施方式仅以蓝牙通信方式进行了举例说明，但其他短距离通信方式均属于本发明保护的范围。

对于无源、无晶振的终端（如智能卡）来说，该终端没有计时功能，而在本实施例中，由于在第一终端与第二终端通信的整个过程中，第一终端始终产生载波信号，因此，本实施例中提出了有别与时钟计时的计时统计方式，本实施例还可以通过计算载波信号的周期个数、脉冲个数以及相位差来统计计时得到的数值，预设数值具体可以包括：预设的载波信号的周期个数、预设的载波信号的脉冲个数以及预设的载波信号的相位差，其中，上述预设的载波信号的周期个数、预设的载波信号的脉冲个数以及预设的载波信号的相位差对应得到的时长均大于第二终端对接收到的第一数据中的待处理数据进行数据处理的时长，此外，可选地，上述预设的周期个数对应的时长、预设的脉冲个数对应的时长、以及预设的相位差对应的时长均可以小于或等于 FWT。作为一种可选的实施方式，预设数值可以包括：预设的周期个数；在步骤 S34 中，第一终端计时得到的数值达到预设数值，包括：第一终端从发送完成第一数据之后持续向第二终端发送的载波信号的周期个数达到预设的周期个数；步骤 S33 中，第二终端计时得到的数值达到预设数值，包括：第二终端从接收完成第一数据之后持续接收到的载波信号的周期个数达到预设的周期个数。

在本实施例中，第一终端始终在产生载波信号，在第一终端需要发送数据时，例如，

第一终端发送第一数据是将第一数据调制在载波信号上发送至第二终端的，在第一终端不需要发送数据时，第一终端发送该载波信号至第二终端，该载波信号上没有携带数据。该可选实施方式中，第一终端与第二终端均具有计数器，可以计算上述情况下载波的周期个数，该可选实施方式提供了一种可选的统计计时得到的数值的方式，第一终端与第二终端无需使用时钟计时，也可以达到精确计时的目的，举例来说，以支持 NFC 通信方式的终端为例，第一终端与第二终端的工作频率为 13.56MHZ，在第一终端与第二终端通信过程中，第一终端（例如读卡器）始终产生 13.56MHz 的载波，载波的时间周期 T 是固定的，T=1/13.56MHz，约等于 74ns，以周期来统计计时得到的数值，单位可以精确到 ns，由此可以达到精确统计的效果，而且，该可选实施方式可以适用于无源无晶振的智能卡。虽然，该可选实施方式仅以 NFC 通信方式进行了举例说明，但其他短距离通信方式均属于本发明保护的范围。

此外，作为另一种本实施例可选的实施方式，预设数值可以包括：预设的脉冲个数；在步骤 S34 中，第一终端计时得到的数值达到预设数值，包括：第一终端从发送完成第一数据之后持续向第二终端发送的载波信号的脉冲个数达到预设的脉冲个数；在步骤 S33 中，第二终端计时得到的数值达到预设数值，包括：第二终端从接收完成第一数据之后持续接收到的载波信号的脉冲个数达到预设的脉冲个数。

统计载波信号的脉冲个数即统计载波信号的峰值的个数，相比于上述统计载波信号的周期个数的方式，统计脉冲个数可以达到进一步精确统计的效果，而且，该可选实施方式可以适用于无源无晶振的智能卡。

此外，作为另一种本实施例可选的实施方式，预设数值可以包括：预设的相位差；在步骤 S34 中，第一终端计时得到的数值达到预设数值，包括：载波信号在第一相位与第二相位的相位差达到预设的相位差，其中，第一相位为载波信号在第一终端发送完成第一数据的时间点的相位，第二相位为载波信号在第一终端允许开始接收第二数据的时间点的相位；在步骤 S33 中，第二终端计时得到的数值达到预设数值，包括：载波信号在第三相位与第四相位的相位差达到预设的相位差，其中，第三相位为载波信号在第二终端在接收完成第一数据的时间点的相位，第四相位为载波信号在第二终端开始发送所述第二数据的时间点的相位。

例如，第一终端与第二终端可以采用之前提到的获得预设数值的方式，协商或一方生成预设的相位差$S = (1/2 + 40)\pi$，在以第一终端为读卡器，第二终端为智能卡为例，读卡器在发送完成第一数据后以及智能卡在接收完成该第一数据后，两者之间的通信波形就是标准的正弦波载波，记录此刻的相位为 0（即第一相位与第三相位为 0），在载波相位差（即第三相位与第四相位的相位差）达到$(1/2 + 40)\pi$时，智能卡发送第二数据，此时，读卡器只有在计时得到的相位差达到$(1/2 + 40)\pi$时允许开始接收且只有接收到第二数据才说明没有出现中间人的劫持的情况，由此，可以识别出中间人的劫持。

在该可选实施方式中，以支持 NFC 通信方式的终端为例，第一终端与第二终端的工作频率为 13.56MHz，在第一终端与第二终端通信过程中，第一终端（例如读卡器）始终产生 13.56MHz 的载波，载波的时间周期是固定的，T=1/13.56MHz，约等于 74ns，相位是可以将一个周期在 2π的角度来划分，以相位来统计计时，单位可以精确到 74/2π ns，相比于上述统计载波信号的周期个数以及脉冲个数的方式，统计相位差可以达到进一步精确统计的效果，而且，该可选实施方式可以适用于无源无晶振的智能卡。虽然，该可选实施方式仅以 NFC 通信方式进行了举例说明，但其他短距离通信方式均属于本发明保护的范围。

通过本发明实施例提供的数据通讯方法，通过第二终端定时发送第一终端定时接收的策略，使得第一终端即使在接收到第二数据的T2<FWT时，仍然可以识别出是否存在中间人劫持的情况，避免用户在毫不知情的情况下造成经济损失。

实施例 4

基于同一发明构思，本发明实施例还提供一种数据通讯系统。可以参见图 6 所示的数据通讯系统，该数据通讯系统包括：第一终端和第二终端，第一终端和第二终端执行如实施例 3 中的数据通讯方法。其中：

第一终端，用于向第二终端发送第一数据，并从发送完成第一数据的时间点开始计时，其中，第一数据至少包括待处理数据；第二终端，用于接收第一数据，并从接收完成第一数据的时间点开始计时；第二终端，还用于在第二终端计时得到的数值达到预设数值时，将第二数据发送至第一终端，其中，第二数据为第二终端对待处理数据进行数据处理后得到的数据；第一终端，还用于在计时得到的数值达到预设数值时，允许开始接收第二数据。

作为一种可选的方式，第一终端与第二终端之间的通信方式包括：短距离无线通信方式。

作为一种可选的方式，第一终端，还用于在第一终端从发送完成第一数据的时间点开始计时之前，与第二终端进行双向的身份认证，在双向的身份认证通过后，与第二终端协商得到传输密钥；

第二终端，还用于生成预设数值，并利用传输密钥对预设数值加密，将加密后的预设数值发送至第一终端；第一终端，还用于利用传输密钥对加密后的预设数值解密得到预设数值，并保存；或者，

第一终端，还用于生成预设数值，并利用传输密钥对预设数值加密，将加密后的预设数值发送至第二终端；第二终端，还用于利用传输密钥对加密后的预设数值解密得到预设数值，并保存。

作为一种可选的方式，第一终端，还用于在第一终端从发送完成第一数据的时间点开始计时之前，与第二终端进行双向的身份认证；

第二终端，还用于在双向的身份认证通过后，生成预设数值，并利用第一终端的公钥对预设数值加密，将加密后的预设数值发送至第一终端；第一终端，还用于利用第一终端

的私钥对加密后的预设数值解密得到预设数值，并保存；

或者，

第一终端，还用于在双向的身份认证通过后，生成预设数值，并利用第二终端的公钥对预设数值加密，将加密后的预设数值发送至第二终端；第二终端，还用于利用第二终端的私钥对加密后的预设数值解密得到预设数值，并保存。

作为一种可选的方式，第一终端，还用于在第一终端向第二终端发送第一数据之前，生成预设数值；第一数据至少还包括：预设数值以及基于预设数值计算得到的防篡改校验值；

第二终端，还用于在接收第一数据之后，还从第一数据中获取预设数值以及防篡改校验值，并对防篡改校验值进行校验，在校验通过后，保存预设数值。

作为一种可选的方式，预设数值包括：预设的时长，预设的时长小于或等于第一终端与第二终端采用的通信协议规定的帧等待时间 FWT；

第一终端计时得到的数值达到预设数值，包括：第一终端从发送完成第一数据之后计时得到的时长达到预设的时长；

第二终端计时得到的数值达到预设数值，包括：第二终端从接收完成第一数据之后计时得到的时长达到预设的时长。

作为一种可选的方式，第一终端，还用于在第一终端与第二终端通信的整个过程中，始终产生载波信号；

预设数值包括：预设的周期个数，预设的周期个数对应的时长小于或等于第一终端与第二终端采用的通信协议规定的 FWT；第一终端计时得到的数值达到预设数值，包括：第一终端从发送完成第一数据之后持续向第二终端发送的载波信号的周期个数达到预设的周期个数；第二终端计时得到的数值达到预设数值，包括：第二终端从接收完成第一数据之后持续接收到的载波信号的周期个数达到预设的周期个数；或者，

预设数值包括：预设的脉冲个数，预设的脉冲个数对应的时长小于或等于第一终端与第二终端采用的通信协议规定的 FWT；其中：第一终端计时得到的数值达到预设数值，包括：第一终端从发送完成第一数据之后持续向第二终端发送的载波信号的脉冲个数达到预设的脉冲个数；第二终端计时得到的数值达到预设数值，包括：第二终端从接收完成第一数据之后持续接收到的载波信号的脉冲个数达到预设的脉冲个数；或者，

预设数值包括：预设的相位差，预设的相位差对应的时长小于或等于第一终端与第二终端采用的通信协议规定的 FWT；其中：第一终端计时得到的数值达到预设数值，包括：载波信号在第一相位与第二相位的相位差达到预设的相位差，其中，第一相位为载波信号在第一终端发送完成第一数据的时间点的相位，第二相位为载波信号在第一终端允许开始接收第二数据的时间点的相位；第二终端计时得到的数值达到预设数值，包括：载波信号在第三相位与第四相位的相位差达到预设的相位差，其中，第三相位为载波信号在第二终端在接收完成第一数据的时间点的相位，第四相位为载波信号在第二终端开始发送第二数

据的时间点的相位。

通过本发明实施例提供的数据通讯系统，通过第二终端定时发送第一终端定时接收的策略，使得第一终端即使在接收到第二数据的 T2<FWT 时，仍然可以识别出是否存在中间人劫持的情况，避免用户在毫不知情的情况下造成经济损失。

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模块、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过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模块中，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模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时，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。

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、一种数据通讯方法，其特征在于，包括：

第一终端向第二终端发送第一数据，并从发送完成所述第一数据的时间点开始计时，其中，所述第一数据至少包括待处理数据；

所述第二终端接收所述第一数据，并从接收完成所述第一数据的时间点开始计时；

当所述第二终端计时得到的数值达到预设数值时，所述第二终端将第二数据发送至所述第一终端，其中，所述第二数据为所述第二终端对所述待处理数据进行数据处理后得到的数据；

所述第一终端计时得到的数值在所述预设数值的有效范围内，则所述第一终端允许开始接收所述第二数据。

2、根据权利要求 1 所述的方法，其特征在于，

所述预设数值的有效范围为$[S, S + 2\Delta S]$，其中，S 为所述预设数值，ΔS由所述第一终端与所述第二终端之间采用的通信方式所支持的最大通信距离确定，其中，$S + 2\Delta S$的和对应的时长小于或等于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FWT。

3、根据权利要求 2 所述的方法，其特征在于，

所述第一终端与所述第二终端之间采用的通信方式包括：短距离无线通信方式。

4、根据权利要求 1 至 3 任一项所述的方法，其特征在于，

在所述第一终端从发送完成所述第一数据的时间点开始计时之前，所述方法还包括：

所述第一终端与所述第二终端进行双向的身份认证，在所述双向的身份认证通过后，所述第一终端与所述第二终端协商得到传输密钥；所述第二终端生成所述预设数值，并利用所述传输密钥对所述预设数值加密，将加密后的预设数值发送至所述第一终端；所述第一终端利用所述传输密钥对所述加密后的预设数值解密得到所述预设数值，并保存；或者，所述第一终端生成所述预设数值，并利用所述传输密钥对所述预设数值加密，将加密后的预设数值发送至所述第二终端；所述第二终端利用所述传输密钥对所述加密后的预设数值解密得到所述预设数值，并保存；或者，

所述第一终端与所述第二终端进行双向的身份认证；在所述双向的身份认证通过后，所述第二终端生成所述预设数值，并利用所述第一终端的公钥对所述预设数值加密，将加密后的预设数值发送至所述第一终端；所述第一终端利用其私钥对所述加密后的预设数值解密得到所述预设数值，并保存；或者，在所述双向的身份认证通过后，所述第一终端生成所述预设数值，并利用所述第二终端的公钥对所述预设数值加密，将加密后的预设数值

发送至所述第二终端；所述第二终端利用其私钥对所述加密后的预设数值解密得到所述预设数值，并保存。

5、根据权利要求 1 至 3 任一项所述的方法，其特征在于，

在所述第一终端向第二终端发送第一数据之前，所述方法还包括：所述第一终端生成所述预设数值；

所述第一数据至少还包括：所述预设数值以及基于所述预设数值计算得到的防篡改校验值；

所述第二终端接收所述第一数据之后，所述方法还包括：

所述第二终端从所述第一数据中获取所述预设数值以及所述防篡改校验值，并对所述防篡改校验值进行校验，在校验通过后，保存所述预设数值。

6、根据权利要求 2 至 5 任一项所述的方法，其特征在于，

所述预设数值包括：预设的时长；所述ΔS为在所述第一终端与所述第二终端之间的距离为两者采用的通信方式所支持的最大通信距离时，所述第一终端传输数据至所述第二终端所需的时长；所述第一终端计时得到的数值在所述预设数值的有效范围内，包括：所述第一终端从发送完成所述第一数据之后计时得到的时长在所述$[S, S + 2\Delta S]$范围内；

所述第二终端计时得到的数值达到所述预设数值，包括：所述第二终端从接收完成所述第一数据之后计时得到的时长达到所述预设的时长；或者，

所述预设数值包括：预设的周期个数；在所述第一终端与所述第二终端通信的整个过程中，所述第一终端始终产生载波信号；所述ΔS为所述载波信号经过所述第一终端与所述第二终端之间采用的通信方式所支持的最大通信距离所产生的周期个数；其中：所述第一终端计时得到的数值在所述预设数值的有效范围内，包括：所述第一终端从发送完成所述第一数据之后持续向所述第二终端发送的所述载波信号的周期个数在所述$[S, S + 2\Delta S]$范围内；

所述第二终端计时得到的数值达到所述预设数值，包括：所述第二终端从接收完成所述第一数据之后持续接收到的所述载波信号的周期个数达到所述预设的周期个数；或者，

所述预设数值包括：预设的脉冲个数；在所述第一终端与所述第二终端通信的整个过程中，所述第一终端始终产生载波信号；所述ΔS为所述载波信号经过所述第一终端与所述第二终端之间采用的通信方式所支持的最大通信距离所产生的脉冲个数；其中：所述第一终端计时得到的数值在所述预设数值的有效范围内，包括：所述第一终端从发送完成所述第一数据之后持续向所述第二终端发送的所述载波信号的脉冲个数在所述$[S, S + 2\Delta S]$范围内；所述第二终端计时得到的数值达到所述预设数值，包括：所述第二终端从接收完成所述第一数据之后持续接收到的所述载波信号的脉冲个数达到所述预设的脉冲个数；或者，

所述预设数值包括：预设的相位差；在所述第一终端与所述第二终端通信的整个过程

中，所述第一终端始终产生载波信号；所述ΔS为所述载波信号经过所述第一终端与所述第二终端之间采用的通信方式所支持的最大通信距离所产生的相位变化值；其中：所述第一终端计时得到的数值在所述预设数值的有效范围内，包括：所述载波信号在第一相位与第二相位的相位差在所述$[S, S + 2\Delta S]$范围内，其中，所述第一相位为所述载波信号在所述第一终端发送完成所述第一数据的时间点的相位，所述第二相位为所述载波信号在所述第一终端允许开始接收所述第二数据的时间点的相位；所述第二终端计时得到的数值达到所述预设数值，包括：所述载波信号在第三相位与第四相位的相位差达到所述预设的相位差，其中，所述第三相位为所述载波信号在所述第二终端在接收完成所述第一数据的时间点的相位，所述第四相位为所述载波信号在所述第二终端开始发送所述第二数据的时间点的相位。

7、根据权利要求 1 至 6 任一项所述的方法，其特征在于，

所述第一终端为读取装置，所述第二终端为应答装置。

8、一种数据通讯系统，包括：如权利要求 1 至 7 中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如权利要求 1 至 7 所述的数据通讯方法。

9、一种数据通讯方法，其特征在于，包括：

第一终端向第二终端发送第一数据，并从发送完成所述第一数据的时间点开始计时，其中，所述第一数据至少包括待处理数据；

所述第二终端接收所述第一数据，并从接收完成所述第一数据的时间点开始计时；

在所述第二终端计时得到的数值达到预设数值时，所述第二终端将第二数据发送至所述第一终端，其中，所述第二数据为所述第二终端对所述待处理数据进行数据处理后得到的数据；

在所述第一终端计时得到的数值达到所述预设数值时，所述第一终端允许开始接收所述第二数据。

10、根据权利要求 9 所述的方法，其特征在于，

所述第一终端与所述第二终端之间的通信方式包括：短距离无线通信方式。

11、根据权利要求 9 或 10 所述的方法，其特征在于，

在所述第一终端从发送完成所述第一数据的时间点开始计时之前，所述方法还包括：

所述第一终端与所述第二终端进行双向的身份认证，在所述双向的身份认证通过后，所述第一终端与所述第二终端协商得到传输密钥；所述第二终端生成所述预设数值，并利用所述传输密钥对所述预设数值加密，将加密后的预设数值发送至所述第一终端；所述第

一终端利用所述传输密钥对所述加密后的预设数值解密得到所述预设数值，并保存；或者，所述第一终端生成所述预设数值，并利用所述传输密钥对所述预设数值加密，将加密后的预设数值发送至所述第二终端；所述第二终端利用所述传输密钥对所述加密后的预设数值解密得到所述预设数值，并保存；或者，

所述第一终端与所述第二终端进行双向的身份认证；在所述双向的身份认证通过后，所述第二终端生成所述预设数值，并利用所述第一终端的公钥对所述预设数值加密，将加密后的预设数值发送至所述第一终端；所述第一终端利用其私钥对所述加密后的预设数值解密得到所述预设数值，并保存；或者，在所述双向的身份认证通过后，所述第一终端生成所述预设数值，并利用所述第二终端的公钥对所述预设数值加密，将加密后的预设数值发送至所述第二终端；所述第二终端利用其私钥对所述加密后的预设数值解密得到所述预设数值，并保存。

12、根据权利要求 9 或 10 所述的方法，其特征在于，

在所述第一终端向第二终端发送第一数据之前，所述方法还包括：所述第一终端生成所述预设数值；

所述第一数据至少还包括：所述预设数值以及基于所述预设数值计算得到的防篡改校验值；

所述第二终端接收所述第一数据之后，所述方法还包括：

所述第二终端从所述第一数据中获取所述预设数值以及所述防篡改校验值，并对所述防篡改校验值进行校验，在校验通过后，保存所述预设数值。

13、根据权利要求 9 至 12 任一项所述的方法，其特征在于，

所述预设数值包括：预设的时长，所述预设的时长小于或等于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 FWT；

所述第一终端计时得到的数值达到预设数值，包括：

所述第一终端从发送完成所述第一数据之后计时得到的时长达到所述预设的时长；

所述第二终端计时得到的数值达到所述预设数值，包括：

所述第二终端从接收完成所述第一数据之后计时得到的时长达到所述预设的时长。

14、根据权利要求 9 至 12 任一项所述的方法，其特征在于，

在所述第一终端与所述第二终端通信的整个过程中，所述第一终端始终产生载波信号；

所述预设数值包括：预设的周期个数，所述预设的周期个数对应的时长小于或等于所述第一终端与所述第二终端采用的通信协议规定的 FWT；其中：所述第一终端计时得到的数值达到预设数值，包括：所述第一终端从发送完成所述第一数据之后持续向所述第二终端发送的所述载波信号的周期个数达到所述预设的周期个数；所述第二终端计时得到的数

值达到所述预设数值，包括：所述第二终端从接收完成所述第一数据之后持续接收到的所述载波信号的周期个数达到所述预设的周期个数；或者，

所述预设数值包括：预设的脉冲个数，所述预设的脉冲个数对应的时长小于或等于所述第一终端与所述第二终端采用的通信协议规定的 FWT；其中：所述第一终端计时得到的数值达到预设数值，包括：所述第一终端从发送完成所述第一数据之后持续向所述第二终端发送的所述载波信号的脉冲个数达到所述预设的脉冲个数；所述第二终端计时得到的数值达到所述预设数值，包括：所述第二终端从接收完成所述第一数据之后持续接收到的所述载波信号的脉冲个数达到所述预设的脉冲个数；或者，

所述预设数值包括：预设的相位差，所述预设的相位差对应的时长小于或等于所述第一终端与所述第二终端采用的通信协议规定的 FWT；其中：所述第一终端计时得到的数值达到预设数值，包括：所述载波信号在第一相位与第二相位的相位差达到预设的相位差，其中，所述第一相位为所述载波信号在所述第一终端发送完成所述第一数据的时间点的相位，所述第二相位为所述载波信号在所述第一终端允许开始接收所述第二数据的时间点的相位；所述第二终端计时得到的数值达到所述预设数值，包括：所述载波信号在第三相位与第四相位的相位差达到预设的相位差，其中，所述第三相位为所述载波信号在所述第二终端在接收完成所述第一数据的时间点的相位，所述第四相位为所述载波信号在所述第二终端开始发送所述第二数据的时间点的相位。

15、根据权利要求 9 至 14 任一项所述的方法，其特征在于，

所述第一终端为读取装置，所述第二终端为应答装置。

16、一种数据通讯系统，包括：如权利要求 9 至 15 中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如权利要求 9 至 15 所述的数据通讯方法。

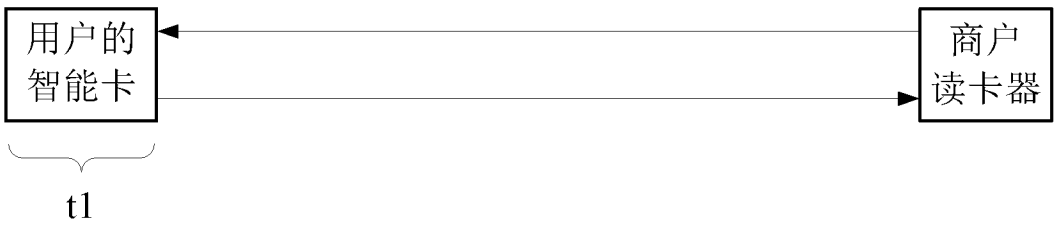
用户的
智能卡
商户
读卡器
t1

图 1

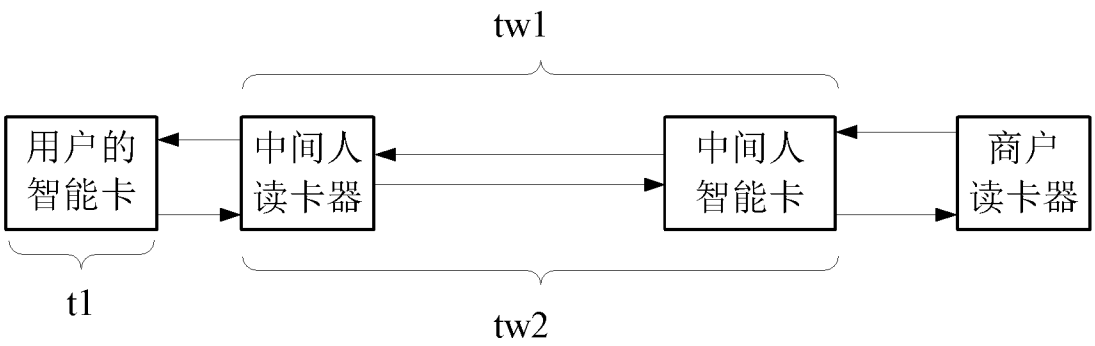
tw1
用户的
智能卡
中间人
读卡器
中间人
智能卡
商户
读卡器
t1
tw2

图 2

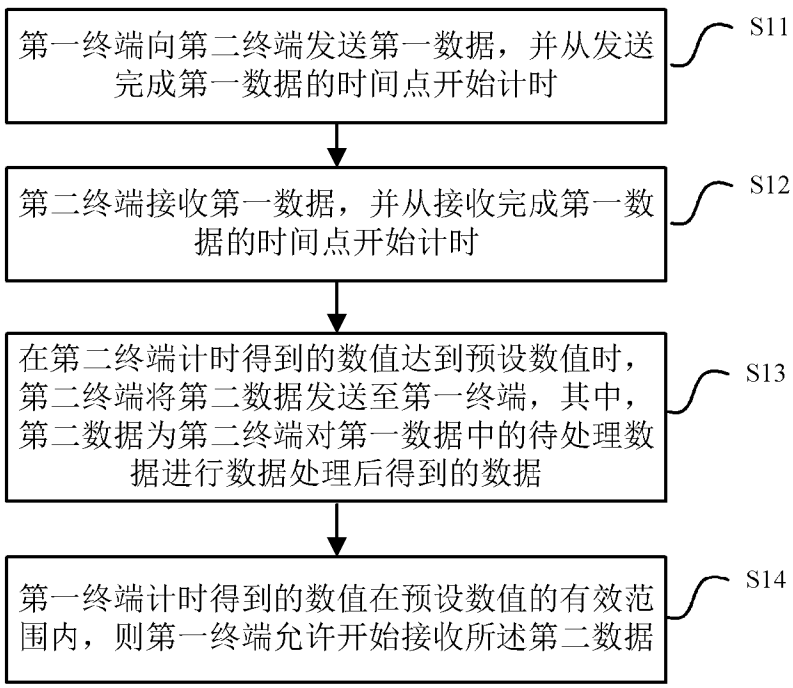
第一终端向第二终端发送第一数据，并从发送完成第一数据的时间点开始计时
S11
第二终端接收第一数据，并从接收完成第一数据的时间点开始计时
S12
在第二终端计时得到的数值达到预设数值时，第二终端将第二数据发送至第一终端，其中，第二数据为第二终端对第一数据中的待处理数据进行数据处理后得到的数据
S13
第一终端计时得到的数值在预设数值的有效范围内，则第一终端允许开始接收所述第二数据
S14

图 3

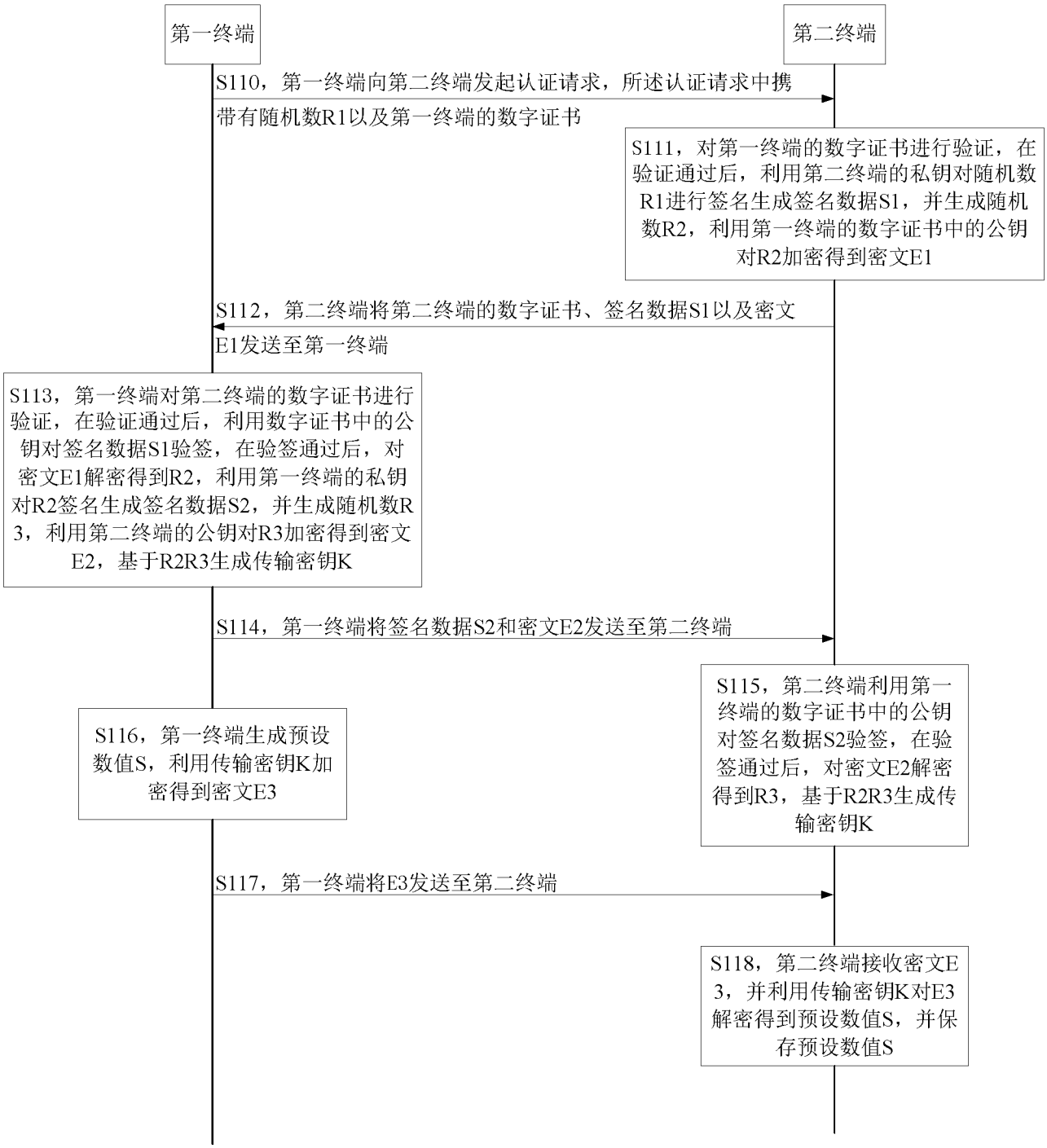
第一终端
第二终端
S110，第一终端向第二终端发起认证请求，所述认证请求中携带有随机数R1以及第一终端的数字证书
S111，对第一终端的数字证书进行验证，在验证通过后，利用第二终端的私钥对随机数R1进行签名生成签名数据S1，并生成随机数R2，利用第一终端的数字证书中的公钥对R2加密得到密文E1
S112，第二终端将第二终端的数字证书、签名数据S1以及密文E1发送至第一终端
S113，第一终端对第二终端的数字证书进行验证，在验证通过后，利用数字证书中的公钥对签名数据S1验签，在验签通过后，对密文E1解密得到R2，利用第一终端的私钥对R2签名生成签名数据S2，并生成随机数R3，利用第二终端的公钥对R3加密得到密文E2，基于R2R3生成传输密钥K
S114，第一终端将签名数据S2和密文E2发送至第二终端
S115，第二终端利用第一终端的数字证书中的公钥对签名数据S2验签，在验签通过后，对密文E2解密得到R3，基于R2R3生成传输密钥K
S116，第一终端生成预设数值S，利用传输密钥K加密得到密文E3
S117，第一终端将E3发送至第二终端
S118，第二终端接收密文E3，并利用传输密钥K对E3解密得到预设数值S，并保存预设数值S

图 4

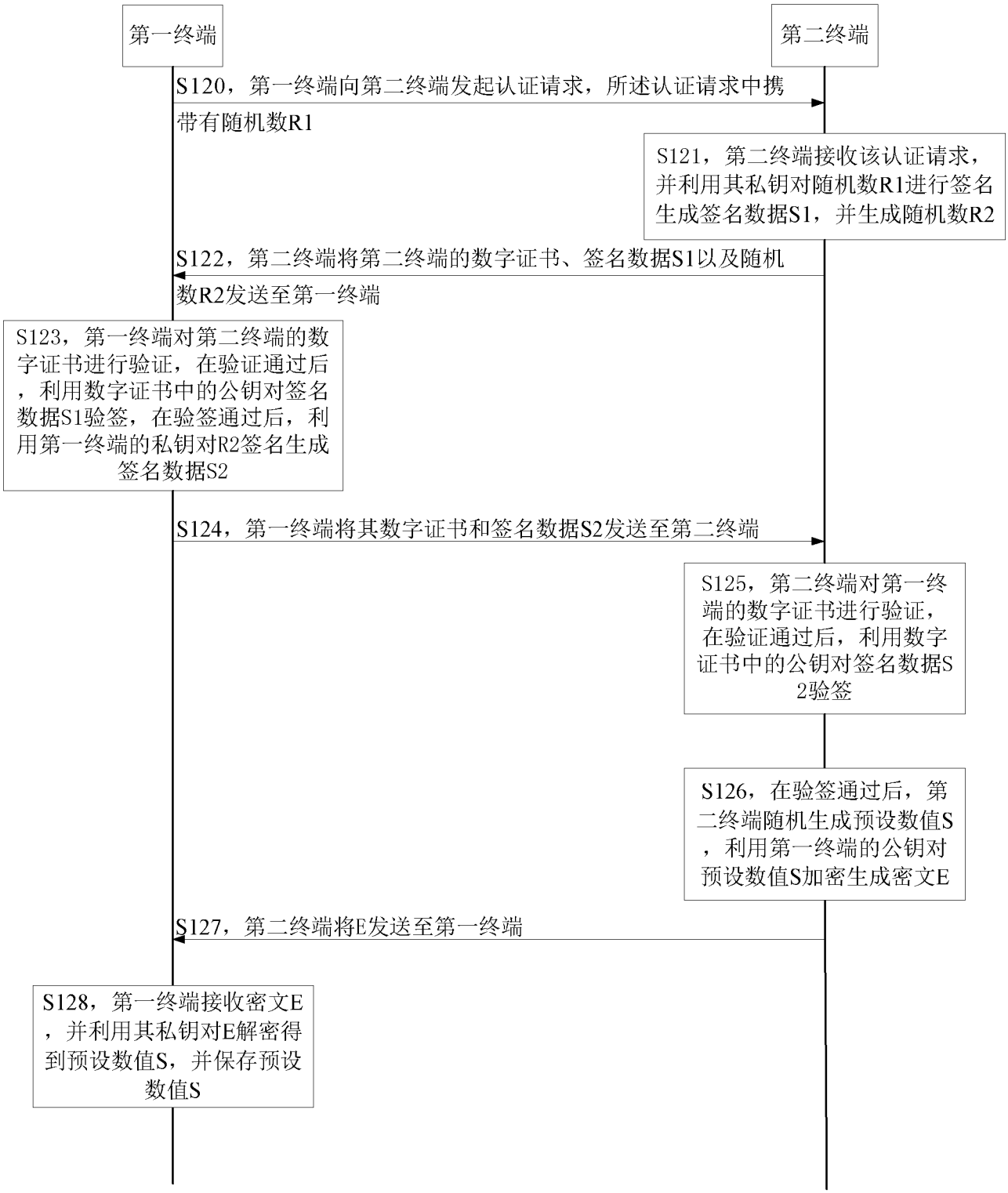
第一终端
第二终端
S120，第一终端向第二终端发起认证请求，所述认证请求中携带有随机数R1
S121，第二终端接收该认证请求，并利用其私钥对随机数R1进行签名生成签名数据S1，并生成随机数R2
S122，第二终端将第二终端的数字证书、签名数据S1以及随机数R2发送至第一终端
S123，第一终端对第二终端的数字证书进行验证，在验证通过后，利用数字证书中的公钥对签名数据S1验签，在验签通过后，利用第一终端的私钥对R2签名生成签名数据S2
S124，第一终端将其数字证书和签名数据S2发送至第二终端
S125，第二终端对第一终端的数字证书进行验证，在验证通过后，利用数字证书中的公钥对签名数据S2验签
S126，在验签通过后，第二终端随机生成预设数值S，利用第一终端的公钥对预设数值S加密生成密文E
S127，第二终端将E发送至第一终端
S128，第一终端接收密文E，并利用其私钥对E解密得到预设数值S，并保存预设数值S

图 5

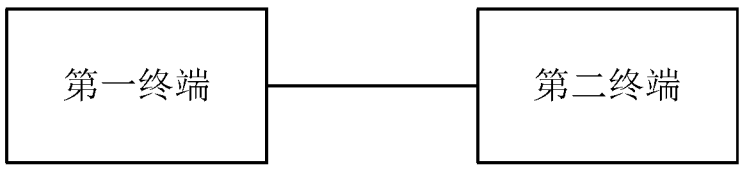
第一终端
第二终端

图 6

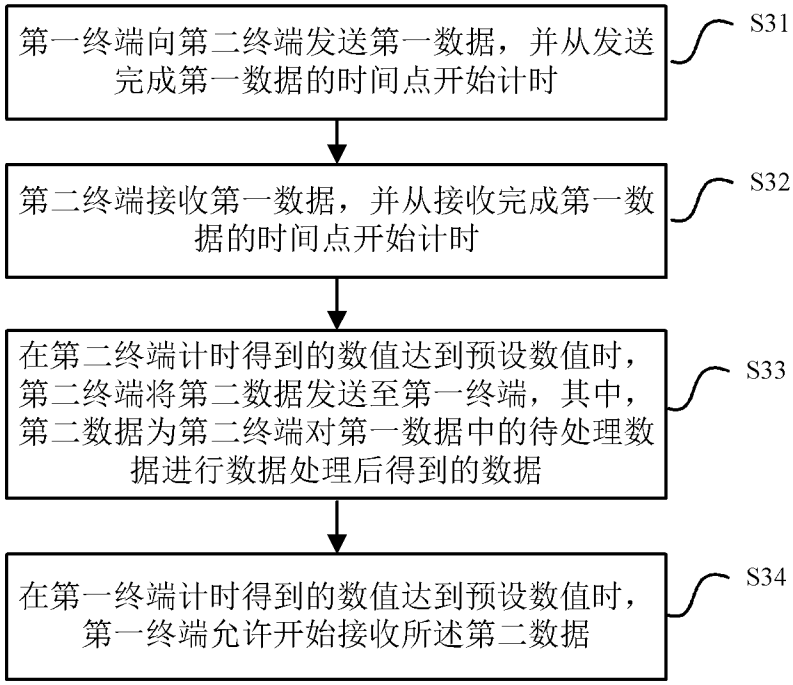
第一终端向第二终端发送第一数据，并从发送完成第一数据的时间点开始计时
S31
第二终端接收第一数据，并从接收完成第一数据的时间点开始计时
S32
在第二终端计时得到的数值达到预设数值时，第二终端将第二数据发送至第一终端，其中，第二数据为第二终端对第一数据中的待处理数据进行数据处理后得到的数据
S33
在第一终端计时得到的数值达到预设数值时，第一终端允许开始接收所述第二数据
S34

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/096025

A. CLASSIFICATION OF SUBJECT MATTER

G06K 7/00 (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)

G06K

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, WPI, EPODOC, IEEE, CNKI: LI, Ming; card reader, card, reader, communication, receive, send, transmit, protocol, time, distance, frame, certification, key, tamper, interception

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104915616 A (FEITIAN TECHNOLOGIES CO., LTD.), 16 September 2015 (16.09.2015), description, paragraphs [0030]-[0031], [0039] and [0070]-[0090], and figure 2	1-16
A	CN 104754501 A (BEIJING YUNJI TECHNOLOGY CO., LTD.), 01 July 2015 (01.07.2015), the whole document	1-16
A	CN 103227816 A (BEIJING XIAOMI TECHNOLOGY CO., LTD.), 31 July 2013 (31.07.2013), the whole document	1-16
A	CN 1936917 A (FEITIAN TECHNOLOGIES CO., LTD.), 28 March 2007 (28.03.2007), the whole document	1-16
A	US 2013136046 A1 (SECUREAU CORPORATION), 30 May 2013 (30.05.2013), the whole document	1-16
A	WO 2014062623 A1 (POWERED CARD SOLUTIONS LLC), 24 April 2014 (24.04.2014), the whole document	1-16

☐ 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
27 October 2017 (27.10.2017)	**03 November 2017 (03.11.2017)**
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 **GAO, Dandan** Telephone No.: (86-10) **62414166**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/096025

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104915616 A	16 September 2015	None	
CN 104754501 A	01 July 2015	None	
CN 103227816 A	31 July 2013	None	
CN 1936917 A	28 March 2007	CN 100414556 C	27 August 2008
US 2013136046 A1	30 May 2013	CA 2857571 A1	06 June 2013
		WO 2013082554 A1	06 June 2013
		EP 2786359 A1	08 October 2014
		US 9414300 B2	09 August 2016
		CN 104040602 A	10 September 2014
		US 2016100368 A1	07 April 2016
WO 2014062623 A1	24 April 2014	US 2015242844 A1	27 August 2015
		JP 2016500173 A	07 January 2016
		KR 20150072438 A	29 June 2015
		CN 104838398 A	12 August 2015
		EP 2907094 A1	19 August 2015

国际检索报告

国际申请号
PCT/CN2017/096025

A. 主题的分类

G06K 7/00(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)

G06K

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, WPI, EPODOC, IEEE, CNKI：李明，读卡器，通信，通讯，接收，发送，协议，时间，距离，帧，认证，密钥，拦截，篡改，card, reader, communication, receive, send, transmit, protocol, time, distance, frame, certification, key, tamper,interception

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	CN 104915616 A (飞天诚信科技股份有限公司) 2015年 9月 16日 (2015-09-16) 说明书第[0030]-[0031]、[0039]、[0070]-[0090]段，附图2	1-16
A	CN 104754501 A (北京云迹科技有限公司) 2015年 7月 1日 (2015-07-01) 全文	1-16
A	CN 103227816 A (北京小米科技有限责任公司) 2013年 7月 31日 (2013-07-31) 全文	1-16
A	CN 1936917 A (北京飞天诚信科技有限公司) 2007年 3月 28日 (2007-03-28) 全文	1-16
A	US 2013136046 A1 (SECUREALL CORPORATION) 2013年 5月 30日 (2013-05-30) 全文	1-16
A	WO 2014062623 A1 (POWERED CARD SOLUTIONS LLC) 2014年 4月 24日 (2014-04-24) 全文	1-16

☐ 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
2017年 10月 27日	2017年 11月 3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 高丹丹 电话号码 (86-10)62414166

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/096025

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	104915616	A	2015年 9月 16日	无			
CN	104754501	A	2015年 7月 1日	无			
CN	103227816	A	2013年 7月 31日	无			
CN	1936917	A	2007年 3月 28日	CN	100414556	C	2008年 8月 27日
US	2013136046	A1	2013年 5月 30日	CA	2857571	A1	2013年 6月 6日
				WO	2013082554	A1	2013年 6月 6日
				EP	2786359	A1	2014年 10月 8日
				US	9414300	B2	2016年 8月 9日
				CN	104040602	A	2014年 9月 10日
				US	2016100368	A1	2016年 4月 7日
WO	2014062623	A1	2014年 4月 24日	US	2015242844	A1	2015年 8月 27日
				JP	2016500173	A	2016年 1月 7日
				KR	20150072438	A	2015年 6月 29日
				CN	104838398	A	2015年 8月 12日
				EP	2907094	A1	2015年 8月 19日