

通信方法及相关装置

技术领域

本申请涉及通信技术、智能汽车技术领域，尤其涉及短距通信技术领域，例如智能汽车、智能家居、智能终端和智能制造等场景中的通信等。具体涉及通信方法及相关装置。

背景技术

在信息化飞速发展的今天，移动终端，手机、平板还是其他可携带式智能终端是我们不可缺少的重要个人智能工具，我们在享受着信息化带来的便利的同时，也面临着安全漏洞和隐私泄露的威胁。以智能汽车为例，随着车辆通信的广泛应用，无线通信也给汽车带来了一系列的安全隐患。例如，通过现有的距离通信技术，黑客可能入侵车载信息系统，获取车辆信息，甚至远程操控汽车，对用户隐私以及车辆安全具有极高的威胁性。

为了保证通信的安全，节点通常都会对传输的数据加密后存储或传输，接收方的节点接收到数据后解密密文，还原明文。具体的，第二节点在接入第一节点时，通常会先确定双方用于通信加密的共享密钥，但是现有的接入过程中，生成的共享密钥的机密性较低。

例如，手机接入无线保真（wireless fidelity，Wi-Fi）设备时，直接输入 8 位的安全参数（此场景中安全参数即为 Wi-Fi 密码），二者就可以得到共享密钥。由于安全参数可能位数较短，或者用户为了方便记忆而使用了比较简单的安全参数，在这些情况下，容易造成设备受到不信任节点的接入，或者基于安全参数生成的密钥可能被破解。不难看出，这样的接入方式容易导致数据泄漏，容易使得用户隐私及安全受到威胁。

因此，如何提高共享密钥的安全性以及避免不可信的攻击者接入是本领域技术人员正在研究的技术问题。

发明内容

本申请实施例提供通信方法及相关装置，能够提高共享密钥的安全性，避免不可信的攻击者接入。

第一方面，本申请实施例提供了一种通信方法，所述方法包括：

接收来自第一节点的第一消息，所述第一消息包含第一密钥协商参数，所述第一密钥协商参数与第一私钥和中间参数相关联，所述中间参数与安全参数和至少一个公共参数相关联，所述安全参数为第一口令或所述第一节点与第二节点之间的预共享密钥 PSK，所述第一口令为所述第一节点与所述第二节点之间的约定接入口令；

向所述第一节点发送第二消息，所述第二消息包含第二密钥协商参数，所述第二密钥协商参数与第二私钥和所述中间参数相关联；

根据所述第一密钥协商参数和所述第二私钥，得到第一密钥。

其中，第一节点和第二节点之间的 PSK 是第一节点与第二节点之间共享的一个秘密值，第一口令可以看作是第一节节点接入第二节节点的密码。第一私钥是与第一节节点相对应的私钥，例如第一节节点可以确定一个随机数作为私钥。第二私钥是与第二节节点相对应的私钥，例如第二节节点可以确定一个随机数作为私钥。

可选的，上述方法可以应用于第二节节点，例如通过第二节节点中的芯片、软件模块实现。

本申请实施例中，先根据安全参数和公共参数得到中间参数，使用中间参数来参与生成第一密钥协商参数。不直接使用安全参数生成密钥，也不直接使用安全参数生成密钥协商参数，因此，即便安全参数的位数较短，也可以通过公共参数来提高安全参数的机密性，从而降低安全参数被破解的可能性。相应提高了第一密钥的安全性，可以降低攻击者接入第二节点的可能性，提升了节点的通信安全性和数据安全性。

在第一方面的一种可能的实施方式中，所述方法还包括：

接收来自所述第一节点的第三消息，所述第三消息包含第一认证信息，所述第一认证信息与第二密钥相关联，所述第二密钥与所述第二密钥协商参数和所述第一私钥相关联；

根据第一密钥验证所述第一认证信息。

本申请实施例中，第一节点所获取的安全参数需要与第二节点中的安全参数一致，如此，第一节点和第二节点可以通过一致的安全参数来参与生成一致的密钥。具体地，在第二节点生成第一密钥时，使用的参数包含第二私钥、安全参数（第一节点中的）、公共参数和第一私钥；在第一节点生成第二密钥时，使用的参数包含第一私钥、安全参数（第二节点中的）、公共参数和第二私钥，由于生成第一密钥和第二密钥的所使用的参数相同，若第一节点和第二节点中的安全参数一致，则生成的第一密钥和第二密钥则一致。

第一节点可以基于第二密钥得到第一认证信息，第二节点基于第一密钥验证认证信息，若验证通过则说明第一密钥和第二密钥一致，即第二节点和第一节点之间具有相同的安全参数，说明第二节点的身份可信。

在攻击者请求接入第二节点时，由于攻击者没有与第二节点一致的安全参数，因此攻击者不能生成与第二节点一致的共享密钥，从而使得攻击者无法接入第二节点，因此可以避免攻击者接入第二节点，防止第二节点与身份不可信的攻击者关联成功。

在第一方面的又一种可能的实施方式中，所述第一密钥用于得到一个或者多个密钥。

作为一种可能的方案，第一密钥用于推演得到加密密钥、完整性密钥、或身份认证密钥等。

这样设置，可以针对不同的场景由第一密钥推演得到专用密钥，避免直接使用第一密钥进行通信，进一步提升了第一密钥的安全性。

在第一方面的又一种可能的实施方式中，所述方法还包括：

如果所述第一认证信息验证通过，向所述第一节点发送关联建立消息。

在上述实施方式中，第一认证信息验证通过，则第一节点得到的第二密钥和第二节点得到的第一密钥一致，从而说明第一节点中的安全参数和第二节点中的安全参数一致，第一节点的身份可信。其中，关联建立消息指示第一节点接入第二成功，或者指示第一节点关联完成。此时，第二节点和第二节点之间可以进行下一步的数据传输操作、或者确定通信密钥、或者完善通信配置信息等。

在第一方面的又一种可能的实施方式中，所述方法还包括：

在所述第三消息的完整性和所述第一认证信息验证通过时，向所述第一节点发送关联建立消息。

上述实施方式中，第二节点可以验证第三消息的消息完整性。在第三消息的完整新验证通过和第一认证信息验证通过的情况下，向所述第一节点发送关联建立消息。

在第一方面的又一种可能的实施方式中，所述方法还包括：

接收所述第一节点发送的密钥协商算法的指示信息，所述密钥协商算法包含双基密码指数函数密钥交换（Two-Basis Password Exponential Key Exchange, TBPEKE）算法。

可选的,所述密钥协商算法的指示信息包含第一密钥协商算法的指示信息,所述第一密钥协商算法的指示信息用于指示 TBPEKE 算法。

其中, TBPEKE 算法是基于椭圆曲线数学理论实现的一种安全算法,可以让通信双方在不安全信道创建起一个密钥,这个密钥可以在后续的通信中作为密钥来加密通信内容。

在上述实施方式中,第一节点和第二节点可能分别支持多种密钥协商算法。在第一节点请求接入第二节点时,第一节点可以在第一消息中向第二节点指示使用何种密钥协商算法,从而使得第一节点和第二节点能够基于一致的密钥协商算法来协商密钥,提升密钥协商效率。

可选的,由于使用的椭圆曲线不同, TBPEKE 算法的数量可以有多个。例如, TBPEKE 算法所使用的椭圆曲线包含以下椭圆曲线中的一项或者多项: SM2 定义的椭圆曲线、或 Curve25519 等。因此, TBPEKE 算法可以包含:使用 SM2 定义的椭圆曲线的 TBPEKE 算法、使用 Curve25519 的 TBPEKE 算法等。应理解,此处是为了方便描述使用不同椭圆曲线的 TBPEKE 算法所做的示例性的描述,具体实施过程中,还可以使用其他椭圆曲线,此处不一一列举。

在第一方面的又一种可能的实施方式中,所述至少一个公共参数包含:第一公共参数和第二公共参数;

其中,所述第一公共参数和所述第二公共参数与所述第一椭圆曲线相关,所述第一椭圆曲线为密钥协商算法对应的椭圆曲线,所述密钥协商算法包含所述 TBPEKE 算法。

在上述实施方式中,公共参数为椭圆曲线中的点,而安全参数是一个秘密值。由于椭圆曲线上的离散对数问题,通过安全参数和公共参数计算得到中间参数是较为容易的,但是,通过获取第一密钥协商参数和公共参数破解安全参数是困难的。因此,通过 TBPEKE 算法和公共参数,可以降低安全参数被破解的可能性,提升节点的安全性。

在第一方面的又一种可能的实施方式中,所述第一公共参数和所述第二公共参数属于所述第一椭圆曲线上的点。

在第一方面的又一种可能的实施方式中,所述第一公共参数为预先定义的,所述第二公共参数通过所述第一公共参数、第一随机数和第二随机数确定,所述第一随机数来自所述第一节点,所述第二随机数来自第二节点。

在第一方面的一种可能的实施方式中,所述至少一个公共参数包含至少一个基点,该至少一个基点属于阶数为 p 的群, p 为素数。

在数学上,群表示一个拥有满足封闭性、满足结合律、有单位元、有逆元的二元运算的代数结构。本申请实施例中,该群相关的运算可以为在第一椭圆曲线上的运算。其中,在椭圆曲线上的运算包含椭圆曲线点乘运算、或椭圆曲线点加运算等中的一项或者多项运算。

可选的,本申请各实施例中,群可以为椭圆曲线的循环子群。

基点,也称生成元,是椭圆曲线密码算法中的参数。基点属于密码算法所选定的椭圆曲线上的点。

一般来说,适用于密码算法的椭圆曲线是定义在有限域内的,因此有限域内的椭圆曲线上的点也是有限的。

阶数是指群中的点的个数,也即是说,阶数为 p 的群中,椭圆曲线上的点的个数为 p 。可选的,群中的任意一个点 A 都满足 $A=d*$ 基点, $*$ 为椭圆曲线点乘运算, d 的取值范围是 $[1, p-1]$ 。

可选的,上述提到的群可以为关于在第一椭圆曲线上的运算的循环群或循环子群。

可选的,部分场景中基点也可以替换为生成元。

在第一方面的又一种可能的实施方式中,当选定的密钥协商算法为 TBPEKE 算法时,至

少一个公共参数包含：阶数为 p 的群中的部分或者全部元素， p 为素数。

其中，阶数为 p 的子群的基点（或称生成元）为 U 。对于选定的一个数 d ， d 的取值范围是 $[1, p-1]$ ，则 dU 包含于该群中。

可选的，至少一个公共参数包含基点 U 。进一步可选的，至少一个公共参数还包含对 U 进行运算得到的 V ， $V=dU$ ， d 的范围是 $[1, p)$ 。

在第一方面的又一种可能的实施方式中，当选定的密钥协商算法为 TBPEKE 算法时，至少一个公共参数包含：阶数为 p 的群中的两个点， p 为素数。

可选的，这两个点可以是两个基点。或者可替换的，两个点中的一个为基点，另一个为根据基点计算得到的第二基点。为了便于描述，本申请统一称为第一基点和第二基点。

在第一方面的又一种可能的实施方式中，当选定的密钥协商算法为 TBPEKE 算法时，TBPEKE 的公共参数包括：阶数为素数 p 的循环群，及群中的两个独立的基点 U 和 V 。

应理解，“独立的”是指 U 和 V 是两个取值不同的点，并不旨在限定 U 和 V 之间没有关联关系。可选的， U 可称为第一基点， V 可称为第二基点。

在第一方面的又一种可能的实施方式中，所述方法还包括：

接收来自所述第一节点的第一计算值，所述第一计算值与第一随机数和第一公共参数相关，所述第一随机数由第一节点确定，所述第一公共参数为预先定义（例如基于 TBPEKE 算法预先定义）；

根据第二随机数和所述第一计算值确定所述第二公共参数；

向所述第一节点发送第二计算值，所述第二计算值与所述第二随机数和所述第一公共参数相关，所述第二计算值用于所述第一节点确定所述第二公共参数。

可选的，所述第一公共参数为前述的第一基点，所述第二公共参数为前述的基点。

在第一方面的又一种可能的实施方式中，所述中间参数满足如下式子：

$$b = U + s * V,$$

其中， b 为所述中间参数， U 、 V 为所述至少一个公共参数， s 为所述安全参数，“*” 为椭圆曲线点乘运算，“+” 为椭圆曲线点加运算。

在第一方面的一种可能的实施方式中， U 为第一基点， V 为第二基点。进一步的， U 、 V 属于阶数为 p 的循环群， p 为素数。

可选的，该群相关的运算为在第一椭圆曲线上的运算。第一椭圆曲线为选定的密钥协商算法所使用的椭圆曲线。示例性地，以选择的密钥协商算法是 TBPEKE 算法为例，第一椭圆曲线可以为：使用 SM2 定义的椭圆曲线、或 Curve25519 等。

在上述实施方式中，中间参数 $(U + s * V)$ 通过安全参数和公共参数的点加和点乘运算得到。

本领域技术人员应知道，对于选定的一条椭圆曲线 $E_p(a,b)$ ，给定标量 k 和点 P （点 P 在椭圆曲线上），计算 $R=k*P$ （* 为椭圆曲线点乘运算）是容易的；但是给定点 P 和点 R （点 P 、点 R 在椭圆曲线上），计算出哪个 k 使得 $kP = R$ 就非常困难。因为实际使用中的椭圆曲线时，原则上把 P 取得相当大， R 也相当大，要把 k 个点逐一算出来与 R 进行比较是数学难题。因此，通过 TBPEKE 算法和公共参数，可以降低安全参数 s 被破解的可能性，提升节点的安全性。

在第一方面的又一种可能的实施方式中，所述第一密钥协商参数 KE_t 满足如下式子：

$$KE_t = SK_t * b,$$

所述第一密钥满足如下式子：

$$\text{第一密钥} = SK_g * KE_t,$$

所述第二密钥协商参数KEg满足如下式子：

$$KEg = SKg * b,$$

所述第二密钥满足如下式子：

$$\text{第二密钥} = SKt * KEg;$$

其中，SKt为所述第一私钥，SKg为所述第二私钥。

由于点乘运算满足结合律，因此第一密钥=SKg*KEt=SKg*(SKt*b)=SKt*(SKg*b)=第二密钥，因此第一节点确定的第一密钥和第二节点确定的第二密钥是相同的。

具体的，第一密钥=SKg*KEt=SKg*(SKt*b)=(SKt.SKg)*(U+s*V)，第二密钥=SKt*KEg=SKt*(SKg*b)=(SKt.SKg)*(U+ s *V)，“.”为乘法运算。因此，第一密钥与第二密钥相同。

上述实施方式给出了一种可能的得到第一密钥协商参数、第二密钥协商参数、第一密钥和第二密钥的方式在生成第一密钥协商参数、第二密钥协商参数时，不直接使用安全参数来计算，而是先根据安全参数和公共参数得到中间参数，使用中间参数来参与生成第一密钥协商参数，从而降低安全参数被破解的可能性，降低攻击者接入第二节点的可能性，提升节点的通信安全性和数据安全性。

在第一方面的又一种可能的实施方式中，所述第一私钥（SKt）的取值范围为[1, p)，所述第二私钥（SKg）的取值范围为[1, p)，其中，p为所述TBPEKE算法所使用的椭圆曲线的阶数。

在第一方面的又一种可能的实施方式中，在所述接收来自第一节点的第一消息之前，所述方法还包括：

广播所述第二节点的密钥协商算法能力，所述第二节点的密钥协商算法能力表征所述第二节点支持的密钥协商算法。

在第一方面的又一种可能的实施方式中，所述第一节点支持的密钥协商算法按优先级顺序排列。

在第一方面的又一种可能的实施方式中，所述第一消息还包括第一新鲜参数，所述第一消息还包括第一新鲜参数，所述第一认证信息与所述第一节点与所述第二节点之间的预共享密钥PSK、所述第二密钥、所述第二消息、所述第一新鲜参数和所述第二节点的密钥协商算法能力相关联。

在第一方面的又一种可能的实施方式中，所述根据所述第一密钥验证所述第一认证信息，包括：

根据所述第一节点与所述第二节点之间的PSK、所述第一密钥、所述第二消息、所述第一新鲜参数和所述第二节点的密钥协商算法能力，验证所述第一认证信息。

在上述实施方式中，参与生成第一认证信息的参数包含第一节点与第二节点之间的PSK、第二密钥、第二消息、第一新鲜参数和第二节点的密钥协商算法能力中的一项或者多项。如此，在验证第一认证信息时，除了第一密钥和第二密钥需要一致，其他参与生成第一认证信息的参数都需要一致才可以验证通过。如此，可以保护上述参数的完整性，降低第二节点被攻击者接入的可能性，提升安全性。

例如，若第一节点发送给第二节点的第一新鲜参数被篡改，则在第二节点验证第一认证信息时所使用的所述第一新鲜参数与第二节点生成第一认证信息时所使用的所述第一新鲜参数则不同，这将导致第一认证信息无法验证通过。

在第一方面的又一种可能的实施方式中，所述第二消息还包括第二认证信息和第二新鲜参数，所述方法还包括：

通过所述第一节点与所述第二节点之间的 PSK、所述第一密钥、所述第二新鲜参数和所述第一消息，得到第二认证信息。

在上述实施方式中，该第二认证信息可以用于第一节点认证第二节点的身份。示例性的，第二节点可以根据相同的参数生成校验信息，若校验信息与第一认证信息相同，则说明第一节点生成的第二密钥和第二节点生成的第一密钥是一致的，从而可以认证第二节点的身份，避免节点与攻击者进行通信，提高节点的安全性。

在第一方面的又一种可能的实施方式中，所述第一消息还包含第一新鲜参数，所述第二消息中还包括第二新鲜参数；所述方法还包括：

根据所述第一密钥、所述第一新鲜参数和所述第二新鲜参数得到第三密钥。

在第一方面的又一种可能的实施方式中，所述 PSK 为预先配置、预先定义或者根据所述第一口令得到的。

在第一方面的又一种可能的实施方式中，所述方法还包括：

根据第一对应关系得到所述第一节点与所述第二节点之间的 PSK。

可以看出，第二节点可以通过对应关系的形式来存储 PSK 与第一节点的对应关系。因此，可以根据对应关系得到第一节点与第二节点之间的 PSK。

在第一方面的又一种可能的实施方式中，所述方法还包括：

根据所述第一口令、第一新鲜参数和第二新鲜参数确定所述第一节点与所述第二节点之间的 PSK。

在一种可能的设计中，PSK 是根据第一口令、第一密钥、第一新鲜参数和第二新鲜参数来确定的。例如，在第一节点与第二节点第一次进行关联时或者第二节点中没有获取到第一节点对应的 PSK 情况下，第二节点可以确定新的 PSK。

第二方面，本申请实施例提供一种通信方法，其特征在于，所述方法包括：

向第二节点发送第一消息，所述第一消息包含第一密钥协商参数，所述第一密钥协商参数与第一私钥和中间参数相关联，所述中间参数与安全参数和至少一个公共参数相关联，所述安全参数为第一口令或第一节点与所述第二节点之间的预共享密钥 PSK，所述第一口令为所述第一节点与所述第二节点之间的约定接入口令；

接收来自所述第二节点的第二消息，所述第二消息包含第二密钥协商参数，所述第二密钥协商参数与第二私钥和所述中间参数相关联；

根据所述第二密钥协商参数和所述第一私钥得到第二密钥。

在第二方面一种可能的实施方式中，所述方法还包括：

向所述第一节点发送第三消息，所述第三消息包含所述第一认证信息，所述第一认证信息与所述第二密钥相关联。

可选的，上述方法可以应用于第一节点，例如通过第一节点中的芯片、软件模块实现。

其中，第一节点和第二节点之间的 PSK 是第一节点与第二节点之间共享的一个秘密值，第一口令可以看作是第一节点接入第二节点的密码。

在第二方面的一种可能的实施方式中，所述第二密钥用于得到一个或者多个密钥。

作为一种可能的方案，第二密钥用于推演得到加密密钥、完整性密钥、或身份认证密钥等。

在第二方面的一种可能的实施方式中，所述方法还包括：

接收来自所述第二节点的关联建立消息。

在第二方面的又一种可能的实施方式中，在向第二节点发送第一消息之前，所述方法还包括：

根据所述第二节点的密钥协商算法能力，选择第一密钥协商算法。其中，第二节点的密钥协商算法能力能够指示第二节点支持的一种或者多种密钥协商算法。

在第二方面的又一种可能的实施方式中，所述方法还包括：

向所述第二节点发送密钥协商算法的指示信息，所述密钥协商算法的指示信息指示双基密码指数函数密钥交换 TBPEKE 算法。

其中，TBPEKE 算法是基于椭圆曲线数学理论实现的一种安全算法，可以让通信双方在不安全信道创建起一个密钥，这个密钥可以在后续的通信中作为密钥来加密通信内容。

可选的，由于使用的椭圆曲线不同，TBPEKE 算法的数量可以有多个。例如，TBPEKE 算法所使用的椭圆曲线包含以下椭圆曲线中的一项或者多项：SM2 定义的椭圆曲线、或 Curve25519 等。因此，TBPEKE 算法可以包含：使用 SM2 定义的椭圆曲线的 TBPEKE 算法、使用 Curve25519 的 TBPEKE 算法等。

在第二方面的又一种可能的实施方式中，所述至少一个公共参数包含：第一公共参数和第二公共参数；

其中，所述第一公共参数和所述第二公共参数与所述第一椭圆曲线相关，所述第一椭圆曲线为密钥协商算法对应的椭圆曲线，所述密钥协商算法包含所述 TBPEKE 算法。

在第二方面的又一种可能的实施方式中，所述第一公共参数和所述第二公共参数属于所述第一椭圆曲线上的点。

在第二方面的又一种可能的实施方式中，所述第一公共参数为预先定义的，所述第二公共参数通过所述第一公共参数、第一随机数和第二随机数确定，所述第一随机数来自所述第一节点，所述第二随机数来自第二节点。

在第二方面的一种可能的实施方式中，所述至少一个公共参数包含至少一个基点，该至少一个基点属于阶数为 p 的群， p 为素数。

可选的，该群可以为关于在第一椭圆曲线上的运算的循环群或循环子群。

可选的，部分场景中基点也可以替换为生成元。

在第二方面的又一种可能的实施方式中，当选定的密钥协商算法为 TBPEKE 算法时，至少一个公共参数包含：阶数为 p 的群中的部分或者全部元素， p 为素数。

其中，阶数为 p 的子群的基点（或称生成元）为 U 。对于选定的一个数 d ， d 的取值范围是 $[1, p-1]$ ，则 dU 包含于该群中。

可选的，至少一个公共参数包含基点 U 。进一步可选的，至少一个公共参数还包含对 U 进行运算得到的 V ， $V=dU$ ， d 的范围是 $[1, p-1]$ 。

在第二方面的又一种可能的实施方式中，当选定的密钥协商算法为 TBPEKE 算法时，至少一个公共参数包含：阶数为 p 的群中的两个点。

可选的，这两个点可以是两个基点。或者可替换的，两个点中的一个为基点，另一个为根据基点计算得到的第二基点。为了便于描述，本申请统一称为第一基点和第二基点。

在第二方面的又一种可能的实施方式中，当选定的密钥协商算法为 TBPEKE 算法时，TBPEKE 的公共参数包括：阶数为素数 p 的循环群，及群中的两个独立的基点 U 和 V 。

应理解，“独立的”是指 U 和 V 是两个取值不同的点，并不旨在限定 U 和 V 之间没有关联关系。

在第二方面的又一种可能的实施方式中，所述方法还包括：

向所述第二节点发送第一计算值，所述第一计算值与第一随机数和第一公共参数相关，所述第一随机数由第一节点确定，所述第一公共参数为预先定义的；

接收来自所述第二节点的第二计算值，所述第二计算值与所述第二随机数和所述第一公共参数相关；

根据第二随机数和所述第一计算值确定所述第二公共参数。

可选的，所述第一公共参数为前述的第一基点，所述第二公共参数为前述的第二基点。

在第二方面的一种可能的实施方式中，所述第一密钥协商算法为所述第一节点支持的密钥协商算法，且所述第一密钥协商算法在所述第二节点支持的密钥协商算法中优先级最高。

在第二方面的一种可能的实施方式中，所述中间参数满足如下式子：

$$b = U + s * V,$$

其中，b 为所述中间参数，U、V 为所述至少一个公共参数，s 为所述安全参数，“*” 为椭圆曲线点乘运算，“+” 为椭圆曲线点加运算。

在第二方面的一种可能的实施方式中，U 为第一基点，V 为第二基点。进一步的，U、V 属于阶数为 p 的群，p 为素数。其中，该群相关的运算为在第一椭圆曲线上的运算。

第一椭圆曲线为选定的密钥协商算法所使用的椭圆曲线。示例性地，以选择的密钥协商算法是 TBPEKE 算法为例，第一椭圆曲线可以为：使用 SM2 定义的椭圆曲线、或 Curve25519 等。

在第二方面的一种可能的实施方式中，所述第一密钥协商参数 K_{Et} 满足如下式子：

$$K_{Et} = SK_t * b,$$

所述第一密钥满足如下式子：

$$\text{第一密钥} = SK_g * K_{Et},$$

所述第二密钥协商参数 K_{Eg} 满足如下式子：

$$K_{Eg} = SK_g * b,$$

所述第二密钥满足如下式子：

$$\text{第二密钥} = SK_t * K_{Eg};$$

其中，SK_t 为所述第一私钥，SK_g 为所述第二私钥。

由于点乘运算满足结合律，因此第一密钥 = SK_g * K_{Et} = SK_g * (SK_t * b) = SK_t * (SK_g * b) = 第二密钥，因此第一节点确定的第一密钥和第二节点确定的第二密钥是相同的。

具体的，第一密钥 = SK_g * K_{Et} = SK_g * (SK_t * b) = (SK_t * SK_g) * (U + s * V)，第二密钥 = SK_t * K_{Eg} = SK_t * (SK_g * b) = (SK_t * SK_g) * (U + s * V)，其中，“.” 为乘法运算。因此，第一密钥与第二密钥相同。

在第二方面的一种可能的实施方式中，所述第一私钥 (SK_t) 的取值范围为 [1, p)，所述第二私钥 (SK_g) 的取值范围为 [1, p)，其中，p 为所述 TBPEKE 算法所使用的椭圆曲线的阶数。

在第二方面的一种可能的实施方式中，在向第二节点发送第一消息之前，所述方法还包括：

接收所述第二节点发送的所述第二节点的密钥协商算法能力，所述第二节点的密钥协商算法能力表征所述第二节点支持的密钥协商算法。

在第二方面的一种可能的实施方式中，所述第一节点支持的密钥协商算法按优先级顺序排列。

在第二方面的一种可能的实施方式中，所述第一消息还包含第一新鲜参数，所述第一消息还包括第一新鲜参数，所述第一认证信息与所述第一节点与所述第二节点之间的预共享密

钥 PSK、所述第二密钥、所述第二消息、所述第一新鲜参数和所述第二节点的密钥协商算法能力相关联。

在第二方面的一种可能的实施方式中，所述第二消息还包括第二认证信息和第二新鲜参数，所述第二认证信息与所述第一节点与所述第二节点之间的 PSK、所述第一密钥、所述第二新鲜参数和所述第一消息相关联。

在第二方面的一种可能的实施方式中，所述方法还包括：

根据所述第一节点与所述第二节点之间的 PSK、所述第二密钥、所述第二新鲜参数和所述第一消息，验证所述第二认证信息；

在所述第二消息的完整性和所述第二认证信息验证通过时，生成所述第一认证信息。

在第二方面的一种可能的实施方式中，所述第一消息中还包含第一新鲜参数，所述第二消息中还包括第二新鲜参数；所述方法还包括：

根据所述第二密钥、所述第一新鲜参数和所述第二新鲜参数得到第四密钥。

在第二方面的一种可能的实施方式中，所述 PSK 为预先配置、预先定义或者根据所述第一口令得到的。

在第二方面的又一种可能的实施方式中，所述方法还包括：

根据第二对应关系得到所述第一节点与所述第二节点之间的 PSK。

可以看出，第一节点可以通过对应关系的形式来存储 PSK 与第二节点的对应关系。因此，可以根据对应关系得到第一节点与第二节点之间的 PSK。

在第二方面的又一种可能的实施方式中，所述方法还包括：

根据所述第一口令、第一新鲜参数和第二新鲜参数确定所述第一节点与所述第二节点之间的 PSK。

在一种可能的设计中，PSK 是根据第一口令、第一密钥、第一新鲜参数和第二新鲜参数来确定的。在第一节点与第二节点第一次进行关联时或者第一节点中没有获取到第二节点对应的 PSK 情况下，第一节点可以确定新的 PSK。

第三方面，本申请实施例提供一种通信装置，所述通信装置包含接收单元、发送单元和处理单元，该通信装置用于实现第一方面任一项实施方式所描述的方法。

在第三方面的一种可能的实施方式中，所述接收单元，用于接收来自第一节点的第一消息，所述第一消息包含第一密钥协商参数，所述第一密钥协商参数与第一私钥和中间参数相关联，所述中间参数与安全参数和至少一个公共参数相关联，所述安全参数为第一口令或所述第一节点与第二节点之间的预共享密钥 PSK，所述第一口令为所述第一节点与所述第二节点之间的约定接入口令；

所述发送单元，还用于向所述第一节点发送第二消息，所述第二消息包含第二密钥协商参数，所述第二密钥协商参数与第二私钥和所述中间参数相关联；

所述处理单元，用于根据所述第一密钥协商参数和所述第二私钥，得到第一密钥。

在第三方面的一种可能的实施方式中，所述接收单元，还用于接收来自所述第一节点的第三消息，所述第三消息包含第一认证信息，所述第一认证信息与第二密钥相关联，所述第二密钥与所述第二密钥协商参数和所述第一私钥相关联；

所述处理单元，还用于根据第一密钥验证所述第一认证信息。

在第三方面的又一种可能的实施方式中，所述第一密钥用于得到一个或者多个密钥。

作为一种可能的方案，第一密钥用于推演得到加密密钥、完整性密钥、或身份认证密钥

等。在第三方面的又一种可能的实施方式中，所述发送单元，还用于：

如果所述第一认证信息验证通过，向所述第一节点发送关联建立消息。

在第三方面的又一种可能的实施方式中，所述发送单元，还用于：

在如果所述第三消息的完整性和所述第一认证信息验证通过时，向所述第一节点发送关联建立消息。

在第三方面的又一种可能的实施方式中，所述接收单元，还用于：

接收所述第一节点发送的密钥协商算法的指示信息，所述密钥协商算法包含 TBPEKE 算法。

可选的，所述密钥协商算法的指示信息包含第一密钥协商算法的指示信息，所述第一密钥协商算法的指示信息用于指示 TBPEKE 算法。

可选的，由于使用的椭圆曲线不同，TBPEKE 算法的数量可以有多个。例如，TBPEKE 算法所使用的椭圆曲线包含以下椭圆曲线中的一项或者多项：SM2 定义的椭圆曲线、或 Curve25519 等。因此，TBPEKE 算法可以包含：使用 SM2 定义的椭圆曲线的 TBPEKE 算法、使用 Curve25519 的 TBPEKE 算法等。

在第三方面的又一种可能的实施方式中，所述至少一个公共参数包含：第一公共参数和第二公共参数；

其中，所述第一公共参数和所述第二公共参数与所述第一椭圆曲线相关，所述第一椭圆曲线为密钥协商算法对应的椭圆曲线，所述密钥协商算法包含所述 TBPEKE 算法。

在第三方面的又一种可能的实施方式中，所述第一公共参数和所述第二公共参数属于所述第一椭圆曲线上的点。

在第三方面的又一种可能的实施方式中，所述第一公共参数为预先定义的，所述第二公共参数通过所述第一公共参数、第一随机数和第二随机数确定，所述第一随机数来自所述第一节点，所述第二随机数来自第二节点。

在第三方面的一种可能的实施方式中，所述至少一个公共参数包含至少一个基点，该至少一个基点属于阶数为 p 的群， p 为素数。

可选的，该群可以为关于在第一椭圆曲线上的运算的循环群或循环子群。

可选的，部分场景中基点也可以替换为生成元。

在第三方面的又一种可能的实施方式中，当选定的密钥协商算法为 TBPEKE 算法时，至少一个公共参数包含：阶数为 p 的群中的部分或者全部元素， p 为素数。

其中，阶数为 p 的子群的基点（或称生成元）为 U 。对于选定的一个数 d ， d 的取值范围是 $[1, p-1]$ ，则 dU 包含于该群中。

可选的，至少一个公共参数包含基点 U 。进一步可选的，至少一个公共参数还包含对 U 进行运算得到的 V ， $V=dU$ ， d 的范围是 $[1, p-1]$ 。

在第三方面的又一种可能的实施方式中，当选定的密钥协商算法为 TBPEKE 算法时，至少一个公共参数包含：阶数为 p 的群中的两个点。

可选的，这两个点可以是两个基点。或者可替换的，两个点中的一个为基点，另一个为根据基点计算得到的第二基点。为了便于描述，本申请统一称为第一基点和第二基点。

在第三方面的又一种可能的实施方式中，当选定的密钥协商算法为 TBPEKE 算法时，TBPEKE 的公共参数包括：阶数为素数 p 的循环群，及群中的两个独立的基点 U 和 V 。

应理解，“独立的”是指 U 和 V 是两个取值不同的点，并不旨在限定 U 和 V 之间没有关联关系。

在第三方面的又一种可能的实施方式中，所述接收单元，还用于接收来自所述第一节点的第一计算值，所述第一计算值与第一随机数和第一公共参数相关，所述第一随机数由第一节点确定，所述第一公共参数为预先定义的；

所述处理单元，还用于根据第二随机数和所述第一计算值确定所述第二公共参数；

所述发送单元，还用于向所述第一节点发送第二计算值，所述第二计算值与所述第二随机数和所述第一公共参数相关，所述第二计算值用于所述第一节点确定所述第二公共参数。

可选的，所述第一公共参数为前述的第一基点，所述第二公共参数为前述的第二基点。

在第三方面的又一种可能的实施方式中，所述至少一个公共参数为两个点，每个点为所述 TBPEKE 算法所使用的椭圆曲线上的一个点。

在第三方面的又一种可能的实施方式中，所述中间参数满足如下式子：

$$b = U + s * V,$$

其中，b 为所述中间参数，U、V 为所述至少一个公共参数，s 为所述安全参数，“*”为椭圆曲线点乘运算，“+”为椭圆曲线点加运算。

在第三方面的一种可能的实施方式中，U 为第一基点，V 为第二基点。进一步的，U、V 属于阶数为 p 的群，p 为素数。其中，该群相关的运算为在第一椭圆曲线上的运算。

第一椭圆曲线为选定的密钥协商算法所使用的椭圆曲线。示例性地，以选择的密钥协商算法是 TBPEKE 算法为例，第一椭圆曲线可以为：使用 SM2 定义的椭圆曲线、或 Curve25519 等。

在第三方面的又一种可能的实施方式中，所述第一密钥协商参数 KEt 满足如下式子：

$$KEt = SKt * b,$$

所述第一密钥满足如下式子：

$$\text{第一密钥} = SKg * KEt,$$

所述第二密钥协商参数 KEg 满足如下式子：

$$KEg = SKg * b,$$

所述第二密钥满足如下式子：

$$\text{第二密钥} = SKt * KEg;$$

其中，SKt 为所述第一私钥，SKg 为所述第二私钥。

由于点乘运算满足结合律，因此第一密钥 = $SKg * KEt = SKg * (SKt * b) = SKt * (SKg * b)$ = 第二密钥，因此第一节点确定的第一密钥和第二节点确定的第二密钥是相同的。

具体的，第一密钥 = $SKg * KEt = SKg * (SKt * b) = (SKt * SKg) * (U + s * V)$ ，第二密钥 = $SKt * KEg = SKt * (SKg * b) = (SKt * SKg) * (U + s * V)$ ，“.”为乘法运算。因此，第一密钥与第二密钥相同。

在第三方面的又一种可能的实施方式中，所述第一私钥 (SKt) 的取值范围为 [1, p)，所述第二私钥 (SKg) 的取值范围为 [1, p)，其中，p 为所述 TBPEKE 算法所使用的椭圆曲线的阶数。

在第三方面的又一种可能的实施方式中，所述发送单元，还用于：

广播所述第二节点的密钥协商算法能力，所述第二节点的密钥协商算法能力表征所述第二节点支持的密钥协商算法。

在第三方面的又一种可能的实施方式中，所述第一节点支持的密钥协商算法按优先级顺序排列。

在第三方面的又一种可能的实施方式中，所述第一消息还包括第一新鲜参数，所述第一消息还包括第一新鲜参数，所述第一认证信息与所述第一节点与所述第二节点之间的预共享

密钥 PSK、所述第二密钥、所述第二消息、所述第一新鲜参数和所述第二节点的密钥协商算法能力相关联。

在第三方面的又一种可能的实施方式中，所述处理单元，还用于：

根据所述第一节点与所述第二节点之间的 PSK、所述第一密钥、所述第二消息、所述第一新鲜参数和所述第二节点的密钥协商算法能力，验证所述第一认证信息。

在第三方面的又一种可能的实施方式中，所述第二消息还包括第二认证信息和第二新鲜参数，所述处理单元，还用于：

通过所述第一节点与所述第二节点之间的 PSK、所述第一密钥、所述第二新鲜参数和所述第一消息，得到第二认证信息。

在第三方面的又一种可能的实施方式中，所述第一消息还包含第一新鲜参数，所述第二消息中还包括第二新鲜参数；所述处理单元，还用于：

根据所述第一密钥、所述第一新鲜参数和所述第二新鲜参数得到第三密钥。

在第三方面的又一种可能的实施方式中，所述 PSK 为预先配置、预先定义或者根据所述第一口令得到的。

在第三方面的又一种可能的实施方式中，所述处理单元，还用于：

根据第一对应关系得到所述第一节点与所述第二节点之间的 PSK。

可以看出，第二节点可以通过对应关系的形式来存储 PSK 与第一节点的对应关系。因此，可以根据对应关系得到第一节点与第二节点之间的 PSK。

在第三方面的又一种可能的实施方式中，所述处理单元，还用于：

根据所述第一口令、第一新鲜参数和第二新鲜参数确定所述第一节点与所述第二节点之间的 PSK。

在一种可能的设计中，PSK 是根据第一口令、第一密钥、第一新鲜参数和第二新鲜参数来确定的。

第四方面，本申请实施例提供一种通信装置，所述通信装置包含发送单元、接收单元和处理单元，该通信装置用于实现第二方面任一项实施方式所描述的方法。

在第四方面的一种可能的实施方式中，所述发送单元，用于向第二节点发送第一消息，所述第一消息包含第一密钥协商参数，所述第一密钥协商参数与第一私钥和中间参数相关联，所述中间参数与安全参数和至少一个公共参数相关联，所述安全参数为第一口令或第一节点与所述第二节点之间的预共享密钥 PSK，所述第一口令为所述第一节点与所述第二节点之间的约定接入口令；

所述接收单元，还用于接收来自所述第二节点的第二消息，所述第二消息包含第二密钥协商参数，所述第二密钥协商参数与第二私钥和所述中间参数相关联；

所述处理单元，用于根据所述第二密钥协商参数和所述第一私钥得到第二密钥。

在第四方面一种可能的实施方式中，

所述发送单元，还用于向所述第一节点发送第三消息，所述第三消息包含所述第一认证信息，所述第一认证信息与第二密钥相关联。

在第四方面的又一种可能的实施方式中，所述第二密钥用于得到一个或者多个密钥。

作为一种可能的方案，第二密钥用于推演得到加密密钥、完整性密钥、或身份认证密钥等。

在第四方面的又一种可能的实施方式中，所述接收单元，还用于：

接收来自所述第二节点的关联建立消息。

在第四方面的又一种可能的实施方式中，所述通信装置还包含处理单元，所述处理单元用于：

根据所述第二节点的密钥协商算法能力，选择第一密钥协商算法。其中，所述第二节点的密钥协商算法能力能够指示第二节点支持的一种或者多种密钥协商算法。

在第四方面的又一种可能的实施方式中，所述发送单元，还用于向所述第二节点发送第一密钥协商的指示信息，所述第一密钥协商算法的指示信息用于指示双基密码指数函数密钥交换 TBPEKE 算法。

可选的，由于使用的椭圆曲线不同，TBPEKE 算法的数量可以有多个。例如，TBPEKE 算法所使用的椭圆曲线包含以下椭圆曲线中的一项或者多项：SM2 定义的椭圆曲线、或 Curve25519 等。因此，TBPEKE 算法可以包含：使用 SM2 定义的椭圆曲线的 TBPEKE 算法、使用 Curve25519 的 TBPEKE 算法等。

在第四方面的又一种可能的实施方式中，所述至少一个公共参数包含：第一公共参数和第二公共参数；

其中，所述第一公共参数和所述第二公共参数与所述第一椭圆曲线相关，所述第一椭圆曲线为密钥协商算法对应的椭圆曲线，所述密钥协商算法包含所述 TBPEKE 算法。

在第四方面的又一种可能的实施方式中，所述第一公共参数和所述第二公共参数属于所述第一椭圆曲线上的点。

在第四方面的又一种可能的实施方式中，所述第一公共参数为预先定义的，所述第二公共参数通过所述第一公共参数、第一随机数和第二随机数确定，所述第一随机数来自所述第一节点，所述第二随机数来自第二节点。

在第四方面的一种可能的实施方式中，所述至少一个公共参数包含至少一个基点，该至少一个基点属于阶数为 p 的群， p 为素数。

可选的，该群可以为关于在第一椭圆曲线上的运算的循环群或循环子群。

可选的，部分场景中基点也可以替换为生成元。

在第四方面的又一种可能的实施方式中，当选定的密钥协商算法为 TBPEKE 算法时，至少一个公共参数包含：阶数为 p 的群中的部分或者全部元素， p 为素数。

其中，阶数为 p 的子群的基点（或称生成元）为 U 。对于选定的一个数 d ， d 的取值范围是 $[1, p-1]$ ，则 dU 包含于该群中。

可选的，至少一个公共参数包含基点 U 。进一步可选的，至少一个公共参数还包含对 U 进行运算得到的 V ， $V=dU$ ， d 的范围是 $[1, p-1]$ 。

在第四方面的又一种可能的实施方式中，当选定的密钥协商算法为 TBPEKE 算法时，至少一个公共参数包含：阶数为 p 的群中的两个点。

可选的，这两个点可以是两个基点。或者可替换的，两个点中的一个为基点，另一个为根据基点计算得到的第二基点。为了便于描述，本申请统一称为第一基点和第二基点。

在第四方面的又一种可能的实施方式中，当选定的密钥协商算法为 TBPEKE 算法时，TBPEKE 的公共参数包括：阶数为素数 p 的循环群，及群中的两个独立的基点 U 和 V 。

应理解，“独立的”是指 U 和 V 是两个取值不同的点，并不旨在限定 U 和 V 之间没有关联关系。

在第四方面的又一种可能的实施方式中，所述发送单元，用于向所述第二节点发送第一计算值，所述第一计算值与第一随机数和第一公共参数相关，所述第一随机数由第一节点确

定, 所述第一公共参数为预先定义的;

所述接收单元, 用于接收来自所述第二节点的第二计算值, 所述第二计算值与所述第二随机数和所述第一公共参数相关;

所述装置还包含处理单元, 处理单元根据第二随机数和所述第一计算值确定所述第二公共参数。

可选的, 所述第一公共参数为前述的第一基点, 所述第二公共参数为前述的第二基点。

在第四方面的又一种可能的实施方式中, 在所述第一密钥协商算法为双基密码指数函数密钥交换 TBPEKE 算法时, 所述至少一个公共参数为两个点, 每个点为所述 TBPEKE 算法所使用的椭圆曲线上的一个点。

在第四方面的又一种可能的实施方式中, 所述第一密钥协商算法为所述第一节点支持的密钥协商算法, 且所述第一密钥协商算法在所述第二节点支持的密钥协商算法中优先级最高。

在第四方面的又一种可能的实施方式中, 所述中间参数满足如下式子:

$$b = U + s * V,$$

其中, b 为所述中间参数, U 、 V 为所述至少一个公共参数, s 为所述安全参数, “*” 为椭圆曲线点乘运算, “+” 为椭圆曲线点加运算。

在第四方面的一种可能的实施方式中, U 为第一基点, V 为第二基点。进一步的, U 、 V 属于阶数为 p 的群, p 为素数。其中, 该群相关的运算为在第一椭圆曲线上的运算。

第一椭圆曲线为选定的密钥协商算法所使用的椭圆曲线。示例性地, 以选择的密钥协商算法是 TBPEKE 算法为例, 第一椭圆曲线可以为: 使用 SM2 定义的椭圆曲线、或 Curve25519 等。

在第四方面的又一种可能的实施方式中, 所述第一密钥协商参数 KEt 满足如下式子:

$$KEt = SKt * b,$$

所述第一密钥满足如下式子:

$$\text{第一密钥} = SKg * KE,$$

所述第二密钥协商参数 KEg 满足如下式子:

$$KEg = SKg * b,$$

所述第二密钥满足如下式子:

$$\text{第二密钥} = SKt * KEg;$$

其中, SKt 为所述第一私钥, SKg 为所述第二私钥。

由于点乘运算满足结合律, 因此第一密钥 = $SKg * KEt = SKg * (SKt * b) = SKt * (SKg * b)$ = 第二密钥, 因此第一节点确定的第一密钥和第二节点确定的第二密钥是相同的。

具体的, 第一密钥 = $SKg * KEt = SKg * (SKt * b) = (SKt * SKg) * (U + s * V)$, 第二密钥 = $SKt * KEg = SKt * (SKg * b) = (SKt * SKg) * (U + s * V)$, “.” 为乘法运算。因此, 第一密钥与第二密钥相同。

在第四方面的又一种可能的实施方式中, 所述第一私钥 (SKt) 的取值范围为 $[1, p)$, 所述第二私钥 (SKg) 的取值范围为 $[1, p)$, 其中, p 为所述 TBPEKE 算法所使用的椭圆曲线的阶数。

在第四方面的又一种可能的实施方式中, 所述接收单元, 还用于:

接收所述第二节点发送的所述第二节点的密钥协商算法能力, 所述第二节点的密钥协商算法能力表征所述第二节点支持的密钥协商算法。

在第四方面的又一种可能的实施方式中, 所述第一节点支持的密钥协商算法按优先级顺序排列。

在第四方面的又一种可能的实施方式中，所述第一消息还包含第一新鲜参数，所述第一消息还包括第一新鲜参数，所述第一认证信息与所述第一节点与所述第二节点之间的预共享密钥 PSK、所述第二密钥、所述第二消息、所述第一新鲜参数和所述第二节点的密钥协商算法能力相关联。

在第四方面的又一种可能的实施方式中，所述第二消息还包括第二认证信息和第二新鲜参数，所述第二认证信息与所述第一节点与所述第二节点之间的 PSK、所述第一密钥、所述第二新鲜参数和所述第一消息相关联。

在第四方面的又一种可能的实施方式中，所述处理单元还用于：

根据所述第一节点与所述第二节点之间的 PSK、所述第二密钥、所述第二新鲜参数和所述第一消息，验证所述第二认证信息；

在所述第二消息的完整性和所述第二认证信息验证通过时，生成所述第一认证信息。

在第四方面的一种可能的实施方式中，所述第一消息中还包含第一新鲜参数，所述第二消息中还包括第二新鲜参数；所述处理单元，还用于：

根据所述第二密钥、所述第一新鲜参数和所述第二新鲜参数得到第四密钥。

在第四方面的一种可能的实施方式中，所述 PSK 为预先配置、预先定义或者根据所述第一口令得到的。

在第四方面的又一种可能的实施方式中，所述处理单元，还用于：

根据第二对应关系得到所述第一节点与所述第二节点之间的 PSK。

在第四方面的又一种可能的实施方式中，所述处理单元，还用于：

根据所述第一口令、第一新鲜参数和第二新鲜参数确定所述第一节点与所述第二节点之间的 PSK。

第五方面，本申请实施例公开了一种通信装置，包括处理器和通信接口，所述通信接口用于接收和/或发送数据，和/或，所述通信接口用于为所述处理器提供输入和/或输出，所述处理器用于调用存储器中存储的计算机程序，以实现第一方面或者第一方面的任意一种可能的实施方式所描述的方法。

第六方面，本申请实施例公开了一种通信装置，包括处理器和通信接口，所述通信接口用于接收和/或发送数据，和/或，所述通信接口用于为所述处理器提供输入和/或输出，所述处理器用于调用存储器中存储的计算机程序，以实现第二方面或者第三方面的任意一种可能的实施方式。

需要说明的是，上述第五方面，和/或，第六方面所描述的通信装置所包含的处理器，可以是专门用于执行这些方法的处理器（便于区别称为专用处理器），也可以是通过调用计算机程序来执行这些方法的处理器，例如通用处理器。可选的，至少一个处理器还可以既包括专用处理器也包括通用处理器。

可选的，上述计算机程序可以存在存储器中。示例性的，存储器可以为非瞬时性（non-transitory）存储器，例如只读存储器（Read Only Memory, ROM），其可以与处理器集成在同一块器件上，也可以分别设置在不同的器件上，本申请实施例对存储器的类型以及存储器与处理器的设置方式不做限定。

在一种可能的实施方式中，上述至少一个存储器位于上述通信装置之外。

在又一种可能的实施方式中，上述至少一个存储器位于上述通信装置之内。

在又一种可能的实施方式之中，上述至少一个存储器的部分存储器位于上述通信装置之

内，另一部分存储器位于上述通信装置之外。

本申请中，处理器和存储器还可能集成于一个器件中，即处理器和存储器还可以被集成在一起。

第七方面，本申请实施例还提供一种芯片系统，所述芯片系统包括至少一个处理器和通信接口，所述通信接口用于发送和/或接收数据，所述至少一个处理器用于调用至少一个存储器中存储的计算机程序，使得所述芯片系统实现第一方面或者第一方面的任意一种可能的实施方式所描述的方法；或者实现第二方面或者第二方面的任意一种可能的实施方式所描述的方法。

第八方面，本申请实施例还提供一种通信系统，该通信系统包括第一节点和第二节点。其中，该第二节点包含上述第三方面或者第三方面的任意一种可能的实施方式所描述的通信装置，或者，该第二节点为实现上述第一方面或者第一方面的任意一种可能的实施方式的节点。该第一节点包含上述第四方面或者第四方面的任意一种可能的实施方式所描述的通信装置，或者，该第一节点为实现上述第二方面或者第二方面的任意一种可能的实施方式的节点。

第九方面，本申请实施例公开了一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机程序，当所述计算机程序在计算机上运行时，使得所述计算机执行第一方面或第一方面的任意一种可能的实施方式所描述的方法，又或者执行第二方面或第二方面的任意一种可能的实施方式所描述的方法。

第十方面，本申请实施例公开了一种计算机程序产品，当所述计算机程序产品在一个或多个处理器上运行时，执行第一方面或第一方面的任意一种可能的实施方式所描述的方法，又或者执行第二方面或第二方面的任意一种可能的实施方式所描述的方法。

第十一方面，本申请实施例公开了一种终端，所述终端可以为智能座舱产品、或者车辆等，所述终端包括第一节点和/或第二节点。

其中，所述第二节点包含上述第三方面或第三方面的任意一种可能的实施方式所描述的装置。

所述第一节点包含上述第四方面或第四方面的任意一种可能的实施方式所描述的通信装置。

可选的，所述第一节点包含摄像头、屏幕、麦克风、音响、雷达、电子钥匙、无钥匙进入、启动系统控制器以及用户设备（user equipment, UE）等模块中的一个或者多个。

可选的，所述第二节点包含网关、基站、汽车座舱域控制器 CDC 等模块中的一个或者多个。可替换的，上述车辆还可以替换为无人机、机器人等智能终端或者运输工具。

本申请第二至第十一方面所提供的技术方案，其有益效果可以参考第一方面的技术方案的有益效果，此处不再赘述。

附图说明

下面将对实施例描述中所需要使用的附图作简单的介绍。

图 1 是本申请实施例提供的一种点加运算的示意图；

图 2 是本申请实施例提供的一种通信系统的示意图；

图 3 是本申请实施例提供的一种通信场景的示意图；

图 4 是本申请实施例提供的一种通信方法的流程示意图；

图 5 是本申请实施例提供的一种确定公共参数的方法流程图；

图 6 是本申请实施例提供的又一种通信方法的流程示意图；

图 7 是本申请实施例提供的又一种通信方法的流程示意图；

图 8 是本申请实施例提供的又一种通信装置的结构示意图；

图 9 是本申请实施例提供的又一种通信装置的结构示意图。

具体实施方式

为了便于理解本申请实施例方案的详细实现，下面先对本申请实施例中涉及的技术术语进行描述。

一.节点 (node)

节点是具有通信能力的电子设备，也称为通信节点。例如，节点可以包括手持终端、车辆、车载设备、或网络侧设备、用户设备、接入终端、用户单元、用户站、移动站、移动台、远方站、远程终端、无线通信设备、用户代理或用户装置等独立设备，也可以是包含在独立设备中的部件（例如芯片或集成电路）。节点可以为任一可能的智能终端设备（如手机）、智能运输设备（如车辆、无人机等）、智能制造设备、智能家居设备（例如大屏、音箱等）等。

示例性地，当节点为车载设备时，可以是汽车座舱（cockpit domain）设备，或者汽车座舱设备中的一个模块，例如：座舱域控制器（cockpit domain controller, CDC）、摄像头、屏幕、麦克风、音响、电子钥匙、无钥匙进入或启动系统控制器等模块中的一个或者多个。在车辆内，节点还可以为电池管理系统和电池包中的电池。

示例性地，当节点为手持终端时，可以是手机（mobile phone）、可穿戴设备、平板电脑（pad）、或带数据收发功能的电脑（如笔记本电脑、掌上电脑等）等。

本申请实施例中的节点可以应用于多种应用场景中，例如以下应用场景：移动互联网（mobile internet, MI）、工业控制（industrial control）、无人驾驶（self driving）、运输安全（transportation safety）、物联网（internet of things, IoT）、智慧城市（smart city）、或智慧家庭（smart home）等。

本申请中的节点可以应用于多种网络类型中，例如应用于以下一种或者多种网络类型中：长期演进（long term evolution, LTE）网络、第五代移动通信技术（5th Generation Mobile Communication Technology, 5G）、无线局域网（例如，Wi-Fi）、蓝牙（Bluetooth, BT）、紫峰（Zigbee）、星闪（SparkLink）、或车载短距无线通信网络等。

在某些应用场景、或某些网络类型中，具备类似通信能力的设备的名称也可能不称为节点，但是为了方便描述，本申请实施例中将具有通信能力的设备统称为节点。

二.安全算法（或称为密码算法）

（1）密钥协商算法

密钥协商是通信双方通过交互一部分参数，从而协商得到密钥的过程。用于密钥协商的算法称为密钥协商算法，也可以称为密钥协商算法。密钥协商算法包含双基密码指数函数密钥交换（Two-Basis Password Exponential Key Exchange, TBPEKE）算法、迪菲赫尔曼密钥交换（Diffie - Hellman key exchange, DH）算法、基于椭圆曲线密码（Elliptic Curve Cryptosystems, ECC）的 DH（ECDH）算法、国密算法（如 SM2 等）、奥克利（Oakley）算法等。

需要说明的是，密钥协商算法也可以看做是一种密钥协商的协议，即，对于通信的双方，密钥协商算法定义了密钥生成和交换的规则。

（2）密钥派生算法（key derivation function, KDF）

密钥派生算法（或称为密钥导出算法）用于从一个秘密值中推演（或称为派生、导出）出一个或多个秘密值。例如，通过秘密值 Key 派生的新的秘密值 DK 可以表示为：DK = K

DF(Key)。当然，此处的 key 仅为示例，具体实施过程中，还可以有其他参数参与密钥派生过程。

本申请实施例中涉及的密钥派生算法可以包含基于密码的密钥派生函数 (password-based key derivation function, PBKDF)、斯克里普特 (scrypt) 算法等。其中，PBKDF 算法又包括第一代 PBKDF1 和第二代 PBKDF2。

应理解，一些 KDF 算法可以通过哈希算法对输入的私密值进行哈希变化，因此 KDF 函数还可以接收算法标识作为输入，用于指示使用何种哈希算法。

需要说明的是，KDF 不仅应用于派生私密值方面，在生成认证信息、身份信息等方面也可以应用。一些可能的实施方式中，在生成认证信息、身份信息时，密钥派生算法也可以称为认证算法 (authentication function, AUF, 或者 AUTH function)，该认证算法用于根据输入的参数得到认证信息。

(3) 加密 (encryption) 算法

加密算法用于保护数据的机密性 (confidentiality)，可以将明文加密得到密文。加密算法可以包括加密运算 (例如椭圆点加运算、或异或运算等)，也可以包括安全性较高的各种数学函数。常见的加密算法主要有异或运算、数据加密标准 (data encryption standard, DES)、三重数据加密算法 (triple data encryption algorithm, 3DES)、高级加密标准 (advanced encryption standard, AES)、RSA 加密算法、数据结构分析算法 (data structure analysis, DSA)、国密算法 (如 SM4 等)、祖冲之算法集 (ZUC 算法，如祖冲之算法、加密算法 128-EEA3 或完整性算法 128-EIA3 等) 等。

三. TBPEKE 算法

本申请实施例中，TBPEKE 算法是基于椭圆曲线数学理论实现的一种安全算法，可以让通信双方在不安全信道创建起一个密钥，这个密钥可以在后续的通信中作为密钥来加密通信内容。可选的，本申请实施例中 TBPEKE 算法所使用的椭圆曲线包含以下椭圆曲线中的一项或者多项：SM2 定义的椭圆曲线、或 Curve25519 等。

下面先对椭圆曲线进行介绍。

椭圆曲线的曲线方程是一个二元三次方程，它有多种形式，最常用的是如下的通用式：

$$E = \{(x, y) \in R | y^2 = x^3 + ax + b, 4a^3 + 27b^2 \neq 0\}$$

从曲线方程易知，椭圆曲线关于 X 轴对称。判定式 $4a^3 + 27b^2 \neq 0$ 可以实现椭圆曲线不存在奇异点，即处处光滑可导，便于进行椭圆曲线上的各类运算：具体如下：

a. 椭圆曲线点加 (point addition) 运算

参见图 1，图 1 是本申请提供的一种可能的点加运算的示意图。参见图 1 的(a)部分，椭圆曲线的加法运算可以通过如下的方式表示：曲线 (图 1 中以 $a=0, b=7$ 的椭圆曲线为例，即： $y^2=x^3+7$) 上标出点 P 和点 Q；做一条经过点 P 和 Q 的直线与曲线相交于第三点 -R；继续做点 -R 关于 X 轴的对称点 R。R 点就是点 P 和 Q 相加得到的点，记作 $P+Q=R$ 。

需要说明的是，椭圆曲线是关于 X 轴对称的，因此 R 是点 -R 的对称点，由于点 -R 在椭圆曲线上，因此点 R 也必然也在椭圆曲线上，即： $P+Q$ 所得到的点在椭圆曲线上。

参见图 1 的(b)部分，当 $P=Q$ 时，则以点 P 作为切点做一条关于椭圆曲线的切线，切线将与椭圆曲线相交与另一点，记做点 -R。同样，做点 -R 的关于 X 轴的对称点 R。这个 R 点就是点 P 和 P 相加得到的点，记作 $P+P=2P=R$ 。

b. 椭圆曲线点减运算

参见图 1 的(c)部分，因 $R - P = R + (-P)$ ，求 $(R - P)$ 就是点 R 与点 -P 的加法运算。而

点-P 就是点 P 对称点。因此，做一条经过点 R 和 -P 的直线，由于椭圆曲线是关于 X 轴对称的，可以看出直线与椭圆曲线相切于点-P，因此做点-P 关于 X 轴的对称点 P，P 点就是点 R 和点-P 相加得到的点。

c. 椭圆曲线点乘 (point multiplication) 运算

将椭圆曲线上的一个点连续相加 n 次，就可以得到 n 次点 P 相加的结果，记为 nP。其中，相加的次数 n 是一个整数，可以称之为标量。椭圆曲线的点乘运算可以称为标量乘 (scalar multiplication) 运算，在涉及多个标量时，可以称为多标量乘运算 (multi-scalar multiplication)。

需要说明的是，点乘算法在不同的运算场景下可能有不同的定义，实现时取决于具体定义。点乘算法的运算规律为准，此处是列举的一种可能的椭圆曲线点乘算法的计算方式。

下面介绍适用于密码算法的椭圆曲线。

上面提供的椭圆曲线是连续的、定义在实数域上的，不适用于在加密过程中使用。因此，密码算法中使用的椭圆曲线通常定义在有限域上，有限域是一个拥有有限元素的集合。通过约束有限域，椭圆上的点能够生成循环子群。

有限域上的椭圆曲线的点加和点乘与实数域上的点加和点乘略有不同，具体可以参考现有技术中的定义。

对于选定的一条椭圆曲线，给定标量 k 和点 G，计算 $R=k*G$ (*为椭圆曲线点乘运算) 是容易的；但是给定点 G 和点 R (点 G、点 R 在椭圆曲线上)，计算出哪个 k 使得 $kG = R$ 就非常困难。因为实际使用中的椭圆曲线时，原则上把 G 取得相当大，R 也相当大，要把 k 个点逐一算出来与 R 进行比较是数学难题。这是椭圆曲线上的离散对数问题。

下面介绍基于 TBPEKE 算法的密钥交换过程。

假设密钥交换双方为第一节点、第二节点，第一节点、第二节点之间有一个互相共享的安全参数 s。TBPEKE 算法所使用的椭圆曲线为 E，U、V 为椭圆曲线 E 上的两个点。在第一节点、第二节点进行密钥交换时，有如下交换步骤：

步骤 1：第一节点计算中间参数 b， $b = (U + s * V)$ ，此处“+”表示椭圆曲线上的点加运算，“*”表示椭圆曲线上的点乘运算，此外，后续式子中“.”表示普通乘法。第一节点生成一个随机数作为第一节点的私钥 SKt，并计算公钥 $PKt = SKt * (U + s * V)$ ，其中公钥 PKt 作为密钥协商参数 KEt。

步骤 2：第一节点将密钥协商参数 KEt 发送给第二节点。

步骤 3：第二节点计算中间参数 b， $b = (U + s * V)$ 。生成一个随机数作为第二节点的私钥 SKg。第二节点计算公钥 $PKg = SKg * (U + s * V)$ ，其中公钥 PKg 作为密钥协商参数 KEg。

步骤 4：第二节点将 KEg 发送给第一节点。

步骤 5：第二节点根据第二节点的私钥和第一节点的公钥得到密钥 K_{KE} ，即：

$$K_{KE} = SKg * KEt = SKg * (SKt * b) = (SKt * SKg) * (U + s * V)。$$

步骤 6：第一节点根据第一节点的私钥和第二节点的公钥得到密钥 K_{KE}' ，即：

$$K_{KE}' = SKt * KEg = SKt * (SKg * b) = (SKt * SKg) * (U + s * V)。$$

而 $K_{KE} = (SKt * SKg) * (U + s * V) = K_{KE}'$ ，即双方得到一致的密钥 K_{KE} 。由于密钥 K_{KE} 没有直接传输，攻击者也难以通过获取的 U、V、KEt、KEg 计算得到 K_{KE} ，因此通过 TBPEKE 算法交换得到的密钥 K_{KE} 具有安全性。

可以理解的，前述的关于算法的解释只是用于简单叙述实现的原理，并不限定使用时一

定使用相同的参数进行实现。算法具体实现过程中还可以有其他的改进和变体，本申请中提到算法可以为经过改进和/或变体后的算法。

四.新鲜参数

新鲜参数是一种信息安全领域中的参数，用于生成密钥和认证参数等，也可以称为新鲜度。新鲜参数可以包括随机数、计数值(counter)、序列号(serial number)、顺序号(sequence number)等中的一个或者多个。不同时刻生成的新鲜参数通常不同。

可以理解的，新鲜参数的具体取值，在每生成一次新鲜参数时会发生变化，从而使得这一次生成密钥(或者认证参数等)所使用的新鲜参数与上一次生成密钥(或者认证参数等)时所使用的新鲜参数不同的，可以提高生成的密钥的安全性。

其中，非重复的随机数值(number once, NONCE)是一个只被使用一次的(非重复的)随机数值。

五.口令

口令可以理解为节点为了让其他节点可以接入从而预先配置或者预先定义的密码，或者理解为两个节点之间约定的秘密值。可选的，口令在形式上可以为数字、字母、符号等其中的一个或者多个组成的字符串(或数字)，可以通过键盘、语音、生物信息等方式输入。例如，手机终端接入支持无线保真(Wireless fidelity, Wi-fi)协议的路由器的场景中，手机终端可以使用“Wi-fi 密码”接入路由器，该“Wi-fi 密码”可以理解为路由器的口令。

为了便于理解，本申请示例性地列举几种可能的口令使用场景(以第一节点请求接入第二节点为例)：

场景 1：第二节点预先定义或者预先配置了第一口令。第一节点的用户可以在第一节点中输入第一口令以接入第二节点。例如，车主通过管理员接口为车辆配置第一口令。当车主的智能手机需要接入车辆时，车主可以在智能手机中输入第一口令，智能手机根据输入的第一口令请求接入车辆。

场景 2：第二节点预先定义或者预先配置第一口令。同样的，第一节点中也预先配置了接入第二节点的第一口令。当需要接入第二节点时，第一节点可以使用预先配置的第一口令进行接入。例如，主机厂在装配车辆时，可以在车辆的 CDC 中配置第一口令，在车辆的雷达中配置 CDC 的第一口令，这样一来，雷达可以使用 CDC 的第一口令来接入 CDC。

场景 3：第三方设备(如网络侧设备、证书中心、认证服务器等等设备，受第二节点信任)可以给第二节点和第一节点分配一个约定值，该约定值可以供第一节点接入第二节点，该约定值可以称为第二节点的接入口令。

需要说明的是，参数与参数之间关联表明参数与参数之间具有联系，例如：参数 A 与参数 B 相关联，说明参数 A 与参数 B 之间存在对应关系(或映射关系)，或者，在参数 A 的计算过程中使用了参数 B(可选还可以使用到其他参数)。

本申请各实施例中提到的“认证”、“校验”、“验证”，可以表征检查是否正确或者合理的意思。本申请各实施例中提到的“接入”表明第一节点与第三节点建立连接的过程。在一些具体的技术场景中，也可以将一个节点“接入”另一个节点的过程，描述为一个节点“关联”另一个节点。

另外，本申请各个实施例中，除特殊说明外，“*”为椭圆曲线点乘运算，“+”为椭圆曲线点加运算，“.”为乘法运算。

下面对本申请实施例的系统架构和业务场景进行描述。需要说明的是，本申请描述的系统架构及业务场景是为了更加清楚的说明本申请的技术方案，并不构成对于本申请提供的技术方案的限定，本领域普通技术人员可知，随着系统架构的演变和新业务场景的出现，本申请提供的技术方案对于类似的技术问题，同样适用。

参见图 2，图 2 是本申请实施例提供的一种可能的通信系统的示意图，该通信系统包括第一节点 201 和第二节点 202。第一节点 201 可以请求关联第二节点 202，关联成功后，第二节点 202 可以与第一节点 201 进行数据传输。

可选的，第二节点 202 与第一节点 201 之间通信的链路可以包括各种类型的连接介质，包括有线链路（例如光纤）、无线链路、或者有线链路和无线链路的组合等。例如可以为近距离连接技术包括星闪（SparkLink）、802.11b/g、蓝牙(blue tooth)、紫蜂(Zigbee)、无线射频识别技术(radio frequency identification, RFID)、超宽带(ultra-wideband, UWB)技术、或无线短距通信系统（例如车载无线短距通信系统）等。再如还可以为远距离连接技术包括基于长期演进（Long Term Evolution, 长期演进）的通信技术、第五代移动通信技术（5th generation mobile networks 或 5th generation wireless systems、5th-Generation, 简称 5G 或 5G 技术）、全球移动通信系统(global System for mobile communications, GSM)、通用分组无线业务(general packet radio Service, GPRS)、通用移动通信系统(universal mobile telecommunications system, UMTS)等无线接入类型技术。

在一些具体的实施场景中，第二节点可以称为 G 节点、控制节点或者接入点（access point）。第一节点可以称为 T 节点或者终端。G 节点向 T 节点的通信链路可以称为 G 链路，T 节点向 G 节点的通信链路可以称为 T 链路。

应理解，本申请各附图中所示的系统仅为示例，其中节点的数量、位置、连接关系为了便于描述而示出的一种可能的情况，不作为对具体通信系统和通信场景的限定。

第二节点 202 和第一节点 201 可以是相同类型的设备，也可以是不同类型的设备。例如，请参见图 3，图 3 是一种可能的通信场景的示意图。车辆的座舱域控制器（cockpit domain controller, CDC）302 是车辆的智能座舱设备中的控制中心，可以看作是第二节点 202。智能手机 301 是具有数据收发能力的设备，可以看作是第一节点 201。

其中，CDC302 可以通过短距通信技术接入，而智能手机 301 支持短距通信技术，因此智能手机 301 可以请求接入该 CDC302。若短距通信技术中通信双方采用数字配对进行接入，则在智能手机 301 中直接点击 CDC302 的标识，通过确认与 CDC302 之间的配对数字，即可通过短距通信技术连接 CDC302。此时，若攻击者冒用智能手机 301 的身份来连接 CDC302，CDC302 难以辨认出攻击者，将导致攻击者成功接入 CDC302，使得车辆的隐私及安全受到威胁。

类似的，在其他的一些场景中，节点也往往难以避免不明身份的攻击者的接入，影响通信的安全。例如，CDC302 支持通过第一口令接入。用户在智能手机 301 中输入口令，CDC302 在确定用户输入的口令正确时，可以进行连接。但是，为了方便输入和记忆，口令通常较短，在通信过程中直接使用口令来得到通信密钥的情况下，攻击者可能会使用暴力破解或离线破解来取得 CDC302 的口令，使得车辆的隐私及安全受到威胁。

有鉴于此，提供本申请实施例的通信方法及装置，可以降低节点与身份不可信的攻击者关联成功的可能性，提升节点安全性。

下面对本申请实施例的方法进行详细介绍。

请参见图 4，图 4 是本申请实施例提供的一种通信方法的流程示意图。可选的，该方法可以基于图 2 所示的通信系统来实现。如图 4 所示的通信方法可以包括步骤 S401 至步骤 S406 中的一个或多个步骤。应理解，本申请为了方便描述，故通过 S401 至 S406 这一顺序进行描述，并不旨在限定一定通过上述顺序进行执行。本申请实施例对于上述一个或多个步骤的执行的先后顺序、执行的时间、执行的次数等不做限定。S401 至步骤 S406 具体如下：

步骤 S401：第一节点向第二节点发送第一消息。相应的，第二节点接收来自第一节点的第一消息。其中，第一消息包含第一密钥协商参数。

具体的，密钥协商参数为密钥协商过程中使用到的参数，为了方便描述，本申请各实施例中将第一节点提供的密钥协商参数称为第一密钥协商参数。

本申请实施例中，第一密钥协商参数与第一私钥和中间参数相关联，该中间参数与安全参数和公共参数相关联。

为了便于理解，下面先对安全参数和公共参数进行介绍。

(1) 安全参数可以包含第一节点与第二节点的共享密钥（包括预共享密钥、对称加密密钥等）、第一口令、第一节点与第二节点之间的预先配置的参数、或通信协议中预先定义的参数等。以预共享密钥（pre-shared key, PSK）为例，预共享密钥是第一节点与第二节点之间共享的一个秘密值。第一节点中可以预先定义、预先配置或者通过互相协商生成等方式得到与第一节点共享的 PSK。

第一口令是第一节点与第二节点之间的约定接入口令，也可以理解为第二节点（或第一节点）为了能够让其他节点接入从而预先配置或者预先定义的密码，或者理解为第一节点与第二节点之间约定的秘密值。第一口令的相关描述还可以参见技术术语解释部分的描述。

作为一种可能的方案，若第一节点中存在与第二节点之间的 PSK，则使用 PSK 作为安全参数。若第一节点中不存在与第二节点之间的 PSK，则以第一口令作为安全参数。即，第一节点优先使用 PSK 来参与密钥协商过程。

第一私钥由第一节点确定，是第一节点的私钥。第一私钥可以是随机数。可选的，在第一节点和第二节点通过 TBPEKE 算法来协商密钥时，第一私钥的取值范围是： $[1, p)$ ，其中， p 为所述 TBPEKE 算法所使用的椭圆曲线的阶数，或者， p 为椭圆曲线相关的群的阶数。应理解，“TBPEKE 算法”本申请实施例示例性提供的一种算法名称，在实施过程中，使用相同或者类似的参数、计算方式的密钥协商算法均落入本申请的范围，尽管其可能不称为“TBPEKE 算法”。

(2) 公共参数是在密钥协商过程中可供多方共同使用的参数。公共参数的数量可以是一个，也可以是多个，以具体实现为准。可选的，当第一节点和第二节点选择不同的密钥协商算法来进行密钥协商时，公共参数的数量和确定方式可能出现不同。

以下列举几种可能的确定公共参数的实现方式：

实现方式一，预先定义或者预先配置公共参数。示例性的，通过协议定义公共参数的数量、及取值等，在第一节点和第二节点通过协议关联时，依据协议定义的公共参数来确定密钥协商参数。示例性的，在通信的多方（例如第一节点和第二节点）中预先配置了公共参数。示例性的，第二节点（或第一节点）中预先配置了公共参数，第二节点可以通过消息发送给其他节点，通信多方基于一致的公共参数来确定密钥协商参数。

实现方式二：由某一节点确定一个参数作为公共参数。公共参数的数量此处不限定。可选的，公共参数的数量也可以是一个，也可以是多个。

例如，第二节点可以生成一个随机数，将该随机数作为公共参数。

再如,第二节点在第一椭圆曲线的群中确定两个点,这两个点作为公共参数。示例性地,第一节点选定一个点作为基点(便于区分称为第一基点),通过对基点进行运算得到第二个点(也可称为第二基点)。

可选的,该群可以为关于在第一椭圆曲线上的运算的群,在椭圆曲线上的运算包含椭圆曲线点乘运算、椭圆曲线点加运算等中的一项或者多项运算。进一步可选的,群对应的阶数为 p , p 可以由节点、标准、厂商或者用户定义。本申请各实施例中的阶数 p 可选为素数。

实现方式三:部分公共参数为预先定义,部分参数由节点确定。

例如,公共参数的数量可以为 2 个,其中一个公共参数为预先定义的,另一个公共参数基于已知的公共参数和第一节点、第二节点分别提供的随机数确定。

作为一种可能的实施方式,当第一节点和第二节点之间的密钥协商算法为 TBPEKE 算法时,至少一个公共参数包含:阶数为 p 的群(或群中的部分元素),和/或,群中的第一基点和第二基点。可选的,该群可以为关于在第一椭圆曲线上的运算的群,在椭圆曲线上的运算包含椭圆曲线点乘运算、椭圆曲线点加运算等中的一项或者多项运算。

作为一种又可能的实施方式,第二节点可以接收来自所述第一节点的第一计算值,第一计算值与第一随机数和第一公共参数相关,第一随机数由第一节点确定(本申请实施例中,确定包含接收得到、拷贝、读取或生成等操作中的一项或者多项)。其中,第一公共参数为预先定义的,例如通过协议规定、厂商配置、用户输入得到的。第二节点根据第二随机数和所述第一计算值确定第二公共参数。第二节点向第一节点发送第二计算值,第二计算值与第二随机数和第一公共参数相关。进一步的,第一节点可以接收来自第一节点的第二计算值,基于第二计算值和第一随机数得到与第一节点一致的第二公共参数。

图 5 所示为本申请实施例提供的一种可能的确定公共参数的流程。其中,公共参数包含两个基点 U 、 V ,其中 U 为预先定义的基点, U 、 V 属于阶数为 p 的循环群, p 为素数。所使用的椭圆曲线可以为选定密钥协商算法定义的椭圆曲线。图 5 所示流程具体可以包含步骤 S51 至步骤 S55,具体如下:

步骤 S51:第一节点生成随机数 x ,计算 $X=x*U$ 。

其中,*为点乘运算。 X 即前述的第一计算值。

步骤 S52:第一节点向第二节点发送 X 。相应的,第二节点接收来自第一节点的 X 。

步骤 S53:第二节点生成随机数 y 、计算 $Y=y*U$ 、计算 $V=y*X$ 。

其中“*”为点乘运算。 Y 即前述的第二计算值, V 为第二基点。可选的,由于 $X=x*U$,因此 $V=y*X=y*(x*U)=(x.y)*U$,“.”为乘法运算。

步骤 S54:第二节点向第一节点发送 Y 。相应的,第一节点接收来自第二节点的 Y 。

步骤 S55:第一节点计算 $V=x*Y$ 。

由于 $Y=y*U$,因此 $V=x*Y=x*(y*U)=(x.y)*U$,“.”为乘法运算。因此,第二节点和第一节点通过图 5 所示的实施例可以确定一致的 V 。需要说明的是,图 5 是为了方便描述,故通过步骤 S51 至步骤 S52 这一顺序描述,本申请对于步骤执行的顺序、执行的实际、执行的次数不做限定。

上面对公共参数和安全参数进行了介绍,下面以密钥协商算法为 TBPEKE 算法为例,提供两种关于第一密钥协商参数的可能方案:

方案一:第一节点基于第一口令 pw 和公共参数(U 和 V)计算中间参数 b ,即: $b=(U+pw*V)$,其中, U 、 V 是位于 TBPEKE 算法所使用的椭圆曲线上的第一基点和第二基点。第一节点生成一个随机数作为第一私钥 SK_t ,并计算第一公钥 PK_t ,其中 $PK_t=SK_t*b=$

$SK_t * (U + pw * V)$ 。该第一公钥 PK_t 作为密钥协商参数 KE_t 。

在一些可能的设计中，位于同一椭圆曲线上的点可以进行点加运算、点乘运算。因此，若某一参数不是椭圆曲线上的点，也可以先将该参数映射为椭圆曲线上的点，然后再进行点加运算（或点乘运算）。以第一私钥 SK_t 为例，一种可能的映射方法如下：第一节点可以将 SK_t 作为横坐标（若超过定义域，则可以将 SK_t 取模），在椭圆曲线上得到映射点 $R(SK_t, y)$ ，后续可以以点 R 来替代 SK_t 。可选的，在一个 SK_t 的值对应有多个 y 值时，可以预先约定 y 值需要满足的条件，从而确定对应的点。

方案二：第一节点基于 PSK 和公共参数（ U 和 V ）计算中间参数 b ，即： $b = (U + PSK * V)$ ，此处 $+$ 表示椭圆曲线上的点加运算， $*$ 表示椭圆曲线上的点乘运算。第一节点生成一个随机数作为第一私钥 SK_t ，并计算第一公钥 PK_t ，其中 $PK_t = SK_t * (U + PSK * V)$ 。该第一公钥 PK_t 作为密钥协商参数 KE_t 。

需要说明的是，这里是为了更清楚的阐述方案，所以上述方案以多个步骤的方式来解释如何得到密钥协商参数 KE_t 。在实际的处理中，也可以是通过一个步骤完成，中间参数、第一公钥等可能只是内部的结果，即密钥协商参数 KE_t 满足： $KE_t = SK_t * (U + s * V)$ 。

可选的，第一节点还可以向第二节点发送密钥协商算法的指示信息，用于指示在密钥协商过程中所使用的算法。其中，该指示信息具体可以通过某一字段（便于描述称为第一字段）指示，例如，第一字段可以是 KE_alg 字段。通过第一字段的取值可以指示第一节点在密钥协商过程中所使用的算法。可选的，密钥协商算法的指示信息还可以包含于前述的第一消息。

请参见表 1，表 1 是本申请实施例提供的一种可能密钥协商算法的指示信息的取值与描述。如表 1 所示，当第一字段的取值为 $0x003$ 时，指示通过 $TBPEKE$ 算法来协商密钥，该 $TBPEKE$ 算法所使用的椭圆曲线是 $SM2$ 算法所定义的椭圆曲线。类似地，当第一字段的取值为 $0x001$ 时，表示第一节点选择 $SM2$ 算法来协商密钥。其余取值情况以此类推，此处不再一一赘述。

表 1 第一字段的可能的取值与描述

值	描述
0x001	SM2
0x002	ECDH，基于 curve25519 的椭圆曲线
0x003	TBPEKE，基于 SM2 的椭圆曲线
0x004	TBPEKE，基于 curve25519 的椭圆曲线
.....	

应理解，表 1 是示例性的字段取值，不表示对指示信息的限定。在具体实施过程中，指示信息的格式、比特数、取值与算法的对应关系也可以有其他设计。

作为一种可能的方案，第二节点可以发送（发送方式可以包含广播发送、组播发送、或单播发送等）其密钥协商算法能力，该密钥协商算法能力用于表征第二节点支持的密钥协商算法。相应的，第一节点根据第二节点支持的密钥协商算法，选择密钥协商算法。第一节点向第二节点发送密钥协商算法的指示信息，用于指示其选择的密钥协商算法。

可选的，第二节点在广播消息（或称为接入消息）中携带其身份和支持的密钥协商算法。其中，密钥协商算法按照优先级顺序排列，例如，优先级高的算法可以排在前面。其中，第二节点的身份包含第二节点的身份标识（identify，ID）、域 ID（domain ID）、媒体存取控制（media access control，MAC）地址、域名、域地址或其他自定义的标识，也称为第二节点

的设备标识。

为了便于理解，以下示例性地提供一种可能的方案，第二节点支持 SM2 算法（标识：0x 001）、ECDH 算法（标识：0x 002）、基于 SM2 的椭圆曲线的 TBPEKE 算法（标识：0x 003）和基于 curve25519 的椭圆曲线的 TBPEKE 算法（标识：0x 004），其优先级分别为 1、2、3、4（数字越大优先级越高）。则广播消息中，第二节点密钥协商算法能力为：“0x 004, 0x 003, 0x 002, 0x 001”。

作为一种可能的方案，所述第一密钥协商算法为所述第一节点支持的密钥协商算法，且第一密钥协商算法在所述第二节点支持的密钥协商算法中优先级最高。例如，第二节点支持的密钥协商算法为：算法 A、算法 B、算法 C 和算法 D 四种算法，其优先级分别为 4、3、2、1（数字越大优先级越高）。而第一节点支持的密钥协商算法为：算法 B、算法 D 和算法 E。第一节点和第二节点均支持的算法为：算法 B、算法 D。由于算法 B 的优先级的最高，因此第一节点选择算法 B 作为密钥协商时使用的算法。

当然，第一节点可以选择第一节点和第二节点均支持的算法中、在第一节点中的优先级最高的算法。例如，第二节点支持的密钥协商算法为：算法 A、算法 B、算法 C 和算法 D 四种算法，其优先级分别为 4、3、2、1（数字越大优先级越高）。而第一节点支持的密钥协商算法为：算法 B、算法 D 和算法 E，其优先级分别为 1、2、3（数字越大优先级越高）。第一节点和第二节点均支持的算法为：算法 B、算法 D。由于在第二节点中，算法 D 的优先级高于算法 B 的优先级，因此第一节点选择算法 D 作为密钥协商时使用的算法。

可选的，对于优先级的设置还可以有其他配置。例如，通过协议规定各种算法的优先级，依据协议规定的优先级来确定使用何种算法。

可选的，第一消息中还可以包含新鲜参数（fresh value），便于区分，以下将第一节点提供的新鲜参数称为第一新鲜参数。其中，新鲜参数包括随机数（例如 NONCE）、计数值、序列号等中的至少一个。本申请各个实施例中，以新鲜参数包含 NONCE 为例进行描述，但本申请对于各种类型的新鲜参数均适用。为了便于说明，第一新鲜参数以 NONCE₁ 来表示。

可选的，第一消息中还包含第一节点的身份。其中，第一节点的身份包含第一节点的 ID、MAC 地址、域名、域地址或其他自定义的标识，也称为第一节点的设备标识。

需要说明的是，具体场景中，第一消息可以称为接入请求消息（或接入请求信息），也可以被称为关联请求消息（或关联请求信息）。本申请各个实施例中不对消息或者信息的名称进行限定，仅对消息内容进行示例性的说明和表达，消息的名称可以进行替换。

应理解，本申请是为了方便描述参数的传递，故以第一消息、第二消息等来作为携带数据的载体。在具体实施过程中，第一消息可以是一条消息，也可以是多条消息，对于第一消息所包含的消息个数可以不限定，类似的，对于后续的第二消息、第三消息所包含的消息的数量也可以不做限定。例如，在第一节点向第二节点发送第一密钥协商参数和第一新鲜参数的时，第一密钥协商参数可以通过消息 1 携带，第一新鲜参数可以通过消息 2 携带，此时，消息 1 和消息 2 包含于第一消息。

步骤 S402：第二节点向第一节点发送第二消息。相应的，第一节点接收来自第二节点的第二消息。其中，第二消息包含第二密钥协商参数。

具体的，本申请各实施例中第二节点提供的密钥协商参数称为第二密钥协商参数。第二密钥协商参数与第二私钥和中间参数相关联，该中间参数与安全参数和公共参数相关联。

其中，第二私钥是第二节点确定的私钥。第二私钥可以是第二节点产生的随机数。可选的，在第一节点和第二节点通过 TBPEKE 算法来协商密钥时，第二私钥的取值范围是： $[1, p)$ ，

其中, p 为所述 TBPEKE 算法所使用的椭圆曲线的阶数, 或者, p 为群的阶数。安全参数、公共参数的详细说明可以参考步骤 S401 中的相关描述。

作为一种可能的方案, 第二密钥协商参数可以通过如下式子表示: $KEg = SKg * b$, 其中, $b = (U + s * V)$, 上述 SKg 为第二私钥, b 为中间参数, U 、 V 为公共参数, s 为安全参数。或者, 第二密钥协商参数通过如下式子表示: $KEg = SKg * (U + s * V)$ 。

可选的, 上述第二消息中还包含新鲜参数。为了方便描述, 本申请各实施例中, 将第二节点提供的新鲜参数称为第二新鲜参数, 部分实施例中使用 $NONCEg$ 表示。

步骤 S403: 第二节点根据所述第一密钥协商参数和所述第二私钥, 得到第一密钥。第一密钥与第一密钥协商参数和第二私钥相关联。

作为一种可能的方案, 第二节点通过如下方式得到第一密钥: 第一密钥 = $SKg * KEt$, 其中 SKg 为第二私钥, KEt 为第一密钥协商参数。由于第一密钥协商参数 KEt 满足如下式子: $KEt = SKt * (U + s * V)$, 第一密钥 K_{KE} 可以满足如下式子:

$$K_{KE} = SKg * KEt = (SKt * SKg) * (U + s * V)。$$

上述为了便于描述, 将确定第一私钥、计算第一密钥的过程分开进行描述。但是在一些具体设计中, 可以将上述计算过程封装为一个计算流程, 该计算流程的输入为第一密钥协商参数, 输出为第一密钥。

可替换的, 上述得到第一密钥的流程由 TBPEKE 算法来指示, 因此上述步骤也可以表述为: 第二节点基于 TBPEKE 算法和第一密钥协商参数得到第一密钥。

可选的, 第一密钥还可以用于得到一个或者多个密钥。作为一种可能的方案, 第一密钥可以用于推演得到加密密钥、完整性密钥、或身份认证密钥等。示例性的, 第二节点可以基于第一密钥计算密钥 Kgt 。例如, $Kgt = KDF(K_{KE}, NONCEt, NONCEg)$, 其中, $NONCEt$ 为第一节点提供的新鲜参数, $NONCEg$ 为第二节点提供的新鲜参数。

作为一种可能的实施方式, 第一密钥可以用于参与生成身份认证信息, 以认证通信双方的身份。

例如, 第二节点可以第一密钥得到第二身份认证信息, 第二认证信息用于认证第二节点的身份, 和/或, 用于验证第一节点和第二节点协商得到密钥是否一致。即: 第二身份认证信息与第一密钥相关联。

在一些可能设计中, 第二认证信息还可以与以下参数关联: 密钥 Kgt 、PSK、第一新鲜参数、第二新鲜参数、第一消息、第二消息中的一项或者多项。上述的消息可以为整条消息, 也可以为消息中的部分数据。以下列举几种可能的第二认证信息的计算方式:

计算方式 1, 第二认证信息 $AUTHg$ 满足: $AUTHg = AUF(K_{KE})$, 其中 K_{KE} 为第一密钥。当然, 除了 K_{KE} , 还可以有其他参数参与生成 $AUTHg$, 如新鲜参数、消息等。示例性的, $AUTHg$ 满足: $AUTHg = AUF(K_{KE}, NONCEg)$, 或满足: $AUTHg = AUF(K_{KE}, NONCEt)$, 或满足: $AUTHg = AUF(K_{KE}, NONCEt, NONCEg)$ 。

计算方式 2, 第二认证信息 $AUTHg$ 满足: $AUTHg = AUF(PSK)$, 这里的 PSK 为第二节点与第一节点之间的 PSK。或者, PSK 也可以为第二节点中存储的, 与第一节点的身份对应的 PSK。

当然, 除了 PSK, 还可以有其他参数参与生成 $AUTHg$, 如新鲜参数、消息等。示例性的, $AUTHg$ 满足: $AUTHg = AUF(PSK, NONCEg)$, 或满足: $AUTHg = AUF(PSK, NONCEt)$, 或满足: $AUTHg = AUF(PSK, NONCEt, NONCEg)$ 。

计算方式 3, 第二认证信息 $AUTHg$ 满足: $AUTHg = AUF(PSK, K_{KE}, NONCEg)$, 第一

消息), 相关参数可以参考前述。

计算方式 4, 由于 AUF 算法的输出值的位数可能较长, 因此, 第二节点可以通过取输出值的部分比特, 使得第二认证信息具有统一的、相对较短的数据位数, 从而可以减小第二消息的数据大小, 提升传输效率。示例性的, $AUTHg = AUF(PSK) \mid_N$ 比特。

其中, N 比特可以由 OEM、生产商、标准或用户来预先定义或预先配置。例如, N 比特可以为高 32 比特, 即 AUTHg 满足: $AUTHg = AUF(PSK, K_{KE}, NONCEg, \text{第一消息}) \mid_{\text{高 } 32 \text{ 比特}}$ 。例如, N 比特可以为低 16 比特, AUTHg 满足: $AUTHg = AUF(PSK, NONCEg) \mid_{\text{低 } 16 \text{ 比特}}$ 。

计算方式 5, 根据第一密钥 K_{KE} 得到认证信息密钥 Kauth, 即: $Kauth = KDF(K_{KE})$, 可选的, 参与生成 Kauth 的参数还可以包含新鲜参数 (例如 NONCEt、或 NONCEg 等)、随机数、PSK、或第一节点的身份等中的一项或者多项。

身份认证密钥可以参与生成得到第二认证信息, 当然, 参与生成第二认证信息的还可以包含其他参数, 如新鲜参数、消息等。作为一种可能的方案, 第二认证信息 AUTHg 满足: $AUTHg = AUF(Kauth, NONCEg, \text{第一消息}) \mid_N$ 比特。

应理解, 本申请的算法中, 参数的顺序仅为示例, 具体实施过程中, 各个参数的输入顺序可以进行变换。可替换的, 上述生成认证信息所使用的 AUF 算法, 也可以替换成其他密码算法, 例如 KDF 算法、加密算法、认证算法等。

在上文中, 第二节点在得到第二认证信息、第二密钥协商参数的一些方案中, 使用到了 PSK。下面示例性地介绍两个获取 PSK 的方式:

方式一: 在第二节点中存在 PSK 与第一节点身份标识的对应关系。即, 在第二节点中, 第一节点与第二节点之间的 PSK 可以对应于第一节点的身份标识。第二节点可以根据第一节点的身份标识和对应关系 (便于区别也可以称为第一对应关系) 获取对应的 PSK。

可选的, PSK 与第一节点的身份标识之间的对应关系, 可以在第二节点中预先配置、预先定义的对应关系, 也可以是第一节点与第二节点通过协商的方式生成 PSK 后保存的对应关系。该对应关系的形式可以是对应关系集合、数据表、数据库等中的一个或者多个, 本申请对此不做限定。参见表 2, 表 2 是本申请实施例提供的一种可能的 PSK 与第一节点身份标识的对应关系集合, 该对应关系集合包括多个第一节点的身份标识、对应的 PSK 以及 PSK 的类型。例如, 对于身份标识为 “ID1” 的第一节点, 第二节点根据临时 ID 为 “ID1.1”, 可以确定其对应的 PSK 为 “PSK1”。进一步的, “PSK1” 的类型是预先配置的。

表 2 PSK 与第二节点的身份标识的对应关系

身份标识	PSK	类型
ID1 (临时 ID1.1)	PSK1	预先配置
ID2 (临时 ID2.1)	PSK2	生成
ID3 (临时 ID3.1)	PSK3	生成

需要说明的是, 在预先配置对应关系的情况下, 第二节点中预先配置的与第一节点之间的 PSK 和第一节点预先配置的与第二节点之间的 PSK 是相同的。在生成 PSK 后保存对应关系的情况下, 第一节点与第二节点生成 PSK 的方法以及所使用的参数也是相同的。

方式二: 第二节点生成与第一节点之间的 PSK。可选的, 生成 PSK 的参数可以包括第一口令、第一新鲜参数、第二新鲜参数、第一节点的身份、或第二节点的身份等中的一项或者

多项。应理解，第二节点和第一节点生成 PSK 的参数应是一致的。

一些场景中，第二消息可以称为安全上下文请求消息（或安全上下文请求信息）。

步骤 S404（可选）：第一节点根据第二密钥协商参数和第一私钥得到第二密钥。

第二密钥与第二密钥协商参数和第一私钥对应，是密钥协商过程中第一节点所获取的密钥。

具体地，第一私钥是第一节点确定的私钥。在步骤 S401 中参与得到了第一密钥协商参数。第一私钥可以是第一节点产生的随机数。可选的，在第一节点和第二节点通过 TBPEKE 算法来协商密钥时，第一私钥的取值范围是：[1, p)，其中，p 为所述 TBPEKE 算法所使用的椭圆曲线的阶数，或者，p 为群的阶数，该群与椭圆曲线相关。

作为一种可能的方案，第一节点通过如下方式得到第二密钥：第二密钥 = SKt * KEg，其中 SKt 为第一私钥，KEg 为第二密钥协商参数。由于第二密钥协商参数 KEg 满足如下式子：KEg = SKg * (U + s * V)，因此，第二密钥 K_{KE}' (为了便于与第一密钥 K_{KE} 区分以下称为 K_{KE}') 可以满足如下式子：

$$K_{KE}' = SKt * KEg = (SKt * SKg) * (U + s * V)。$$

由于 K_{KE} = (SKt * SKg) * (U + s * V) = K_{KE}'，因此第一节点和第二节点通过交换密钥协商参数得到了一致的密钥 K_{KE}。

上述为了便于描述，将确定第二私钥、计算第二密钥的过程分开进行描述。但是在一些具体设计中，可以将上述计算过程封装为一个计算流程，该计算流程的输入为第二密钥协商参数，输出为第二密钥。

作为又一种可能的方案，上述得到第二密钥的流程由 TBPEKE 算法来指示，因此上述步骤也可以表述为：第一节点基于 TBPEKE 算法和第二密钥协商参数得到第二密钥。

可选的，第二密钥可以用于得到一个或者多个密钥。作为一种可能的方案，第二密钥可以用于得到加密密钥、完整性密钥、身份认证密钥等。

例如，第一节点可以基于第二密钥计算得到密钥 K_{gt}。例如，K_{gt} = KDF (K_{KE}', NONCEt, NONCEg)，其中，NONCEt 为第一节点提供的新鲜参数，NONCEg 为第二节点提供的新鲜参数。

作为一种可能的实施方式，第一密钥可以用于参与生成身份认证信息，以认证通信双方的身份。示例性的，如步骤 S405 和步骤 S406 所示。

步骤 S405（可选）：第一节点向第二节点发送第三消息。相应的，第二节点接收来自第一节点的第三消息。其中，第三消息包含第一认证信息。

第一认证信息用于认证第一节点的身份，和/或，用于第二节点验证第二节点和第一节点协商得到密钥是否一致。第一认证信息与第二密钥相关联。

在一些可能设计中，参与生成第一认证信息的可选参数还可以包括密钥 K_{gt}、PSK、第一新鲜参数、第二新鲜参数、第一消息、第二消息中的一项或者多项。上述的消息可以为整条消息，也可以为消息中的部分数据。以下列举几种可能的第一认证信息的计算方式：

计算方式 1，第一认证信息 AUTHt 满足：AUTHt = AUF (K_{KE}'), 其中 K_{KE}' 为第二密钥。当然，除了 K_{KE}，还可以有其他参数参与生成 AUTHt，如新鲜参数、消息等。示例性的，AUTHt 满足：AUTHt = AUF (K_{KE}', NONCEt)，或满足：AUTHt = AUF (K_{KE}', NONCEg)，或满足：AUTHt = AUF (K_{KE}', NONCEt, NONCEg)。

计算方式 2，第一认证信息 AUTHt 满足：AUTHt = AUF (PSK)，这里的 PSK 为第二节点与第一节点之间的 PSK。或者，PSK 也可以为第一节点中存储的，与第二节点的身份对应

的 PSK。

当然，除了 PSK，还可以有其他参数参与生成 AUTHt，如新鲜参数、消息等。示例性的，AUTHt 满足：AUTHt = AUF (PSK, NONCEg)，或满足：AUTHt = AUF (PSK, NONCEt)，或满足：AUTHt = AUF (PSK, NONCEt, NONCEg)。

计算方式 3，第一认证信息 AUTHt 满足：AUTHt = AUF (PSK, K_{KE}' ，第二消息，NONCEt，第一节节点的密钥协商算法能力)，相关参数可以参考前述。

计算方式 4，由于 AUF 算法的输出值的位数可能较长，因此，第一节节点可以通过取输出值的部分比特，使得第一认证信息具有统一的、相对较短的数据位数，从而可以减小第三消息的数据大小，提升传输效率。示例性的，AUTHt = AUF (PSK) |_{N 比特}。

其中，N 比特可以由 OEM、生产商、标准或用户来预先定义或预先配置。例如，N 比特可以为高 32 比特，即 AUTHt 满足：AUTHt = AUF (PSK, K_{KE}' ，第二消息，NONCEt，第一节节点的密钥协商算法能力) |_{高 32 比特}。例如，N 比特可以为低 16 比特，AUTHt 满足：AUTHt = AUF (PSK, NONCEg) |_{低 16 比特}。

计算方式 5，根据第二密钥 K_{KE}' 得到认证信息密钥 Kauth，即：Kauth = KDF (K_{KE}')，可选的，参与生成 Kauth 的参数还可以包含新鲜参数（例如 NONCEt、或 NONCEg 等）、随机数、PSK、或第一节节点的身份等中的一项或者多项。

身份认证密钥可以参与生成得到第一认证信息，当然，参与生成第一认证信息的还可以包含其他参数，如新鲜参数、消息等。作为一种可能的方案，第一认证信息 AUTHt 满足：AUTHt = AUF (Kauth, NONCEt, 第二消息，第一节节点的密钥协商算法能力) |_{N 比特}。

可替换的，上述生成认证信息所使用的 AUF 算法，也可以替换成其他密码算法，例如 KDF 算法、加密算法、认证算法等。

可选的，在第二消息包含第二认证信息 AUTHg 的情况下，第一节节点可以根据第二密钥验证第二认证信息 AUTHg。如果第一节节点验证第二认证信息 AUTHg 正确时，则第一节节点生成第一认证信息 AUTHt。

作为一种可能的方案，第二节节点使用什么参数生成 AUTHg，第二节节点也使用自身获取的相同的参数来生成校验信息。若校验信息与 AUTHg 一致，则第一节节点验证第二认证信息 AUTHg 正确。若校验信息与 AUTHg 不一致，则第一节节点验证第二认证信息 AUTHg 不通过。

进一步的，第二消息中还可以包含完整性验证信息，第一节节点可以根据完整性验证信息验证第二信息的完整性。如果第二消息的完整性和第二认证信息验证通过，则第一节节点生成认证信息 AUTHt。

其中，第一节节点获取 PSK 的方式可以是通过对应关系获取、或者通过参数生成 PSK。相关描述可以参见步骤 S402 中第二节节点侧的描述，此处不在赘述。

一些场景中，第三消息可以称为安全上下文响应消息（或安全上下文响应信息）。

步骤 S406（可选）：第二节节点根据第一密钥验证第一认证信息。

在一种可选的方案中，第一节节点使用什么参数生成第一认证信息，则第二节节点也应当使用相同的参数生成校验信息，如果校验信息与第一认证信息相同，则验证通过。

例如，若第一认证信息 AUTHt 满足：AUTHt = AUF (PSK, K_{KE}' , NONCEt, 第二消息) |_{高 32 比特}，则第二节节点生成校验信息 check1 = AUF (PSK, K_{KE} , NONCEt, 第二消息) |_{高 32 比特}，若校验信息 check1 与 AUTHt 相同，则验证通过。

作为一种可能的方案，如果第一认证信息验证通过，第二节节点向第一节节点发送关联建立消息。相应的，第一节节点接收关联建立消息，可以与第二节节点建立关联。

作为又一种可能的方案,如果第一认证信息验证不通过,第二节点可以断开与第一节点之间的通信连接、丢弃第一消息、或丢弃第三消息等。例如,若第一认证信息验证不通过,说明第二节点中的第一密钥 K_{KE} 与第一节点的第二密钥 K_{KE}' 不同,因此第一节点的身份不可信,第一节点可能是攻击者伪装的节点,故断开与第一节点之间的通信连接,避免接入不可信的节点。

可选的,上述第一消息、第二消息、第三消息、关联建立消息等中的一个或者多个消息中可以包含消息认证码(Message authentication code, MAC)。该消息认证码是经过特定算法后产生的信息(或一小段信息),可以用于检查某段消息的完整性,可选的,还可以身份验证。因此,接收方可以根据消息认证码检查消息完整性。

可选的,在第二节点确定了加密密钥的情况下,该关联建立消息还可以通过加密密钥进行加密得到密文。相应的,第二节点中也确定与加密密钥对应的解密密钥,该解密密钥可以对密文进行解密从而获取关联建立消息的内容。

在图4所示的实施例中,第二节点先根据安全参数和公共参数得到中间参数,使用中间参数来参与生成第一密钥协商参数。不直接使用安全参数生成密钥,也不直接使用安全参数生成密钥协商参数,因此,即便安全参数的位数较短,也可以通过公共参数来提高安全参数的机密性,从而降低安全参数被破解的可能性。相应提高了第一密钥的安全性,可以降低攻击者接入第二节点的可能性,提升了节点的通信安全性和数据安全性。

进一步的,第一节点所获取的安全参数需要与第二节点中的安全参数一致,如此,第一节点和第二节点可以通过一致的安全参数来参与生成一致的密钥。具体地,在第二节点生成第一密钥时,使用的参数包含第二私钥、安全参数(第一节点中的)、公共参数和第一私钥;在第一节点生成第二密钥时,使用的参数包含第一私钥、安全参数(第二节点中的)、公共参数和第二私钥,由于生成第一密钥和第二密钥的所使用的参数相同,若第一节点和第二节点中的安全参数一致,则生成的第一密钥和第二密钥则一致。

第一节点可以基于第二密钥得到第一认证信息,第二节点基于第一密钥验证认证信息,若验证通过则说明第一密钥和第二密钥一致,即第二节点和第一节点之间具有相同的安全参数,说明第二节点的身份可信。

在攻击者请求接入第二节点时,由于攻击者没有与第二节点一致的安全参数,因此攻击者不能生成与第二节点一致的共享密钥,从而使得攻击者无法接入第二节点,因此可以避免攻击者接入第二节点,防止第二节点与身份不可信的攻击者关联成功。

以上图4所示的方法实施例中包含了很多可能的实现方案,下面结合图6、图7对其中的部分实现方案进行举例说明,需要说明的是,图5未解释到的相关概念、操作或者逻辑关系可以参照图4所示实施例中的相应描述。

请参见图6,图6是本申请实施例提供的一种可能的通信方法的方法流程图。进一步的,该方法可以基于图2所示的架构来实现。如图6所示的通信方法可以包括步骤S601至步骤S611。应理解,本申请为了方便描述,故通过S601至S611这一顺序进行描述,并不旨在限定一定通过上述顺序进行执行。本申请实施例对于上述一个或多个步骤的执行的先后顺序、执行的时间、执行的次数等不做限定。S601至步骤S611具体如下:

步骤S601:第一节点选择TPPEKE算法。

具体地,第一节点从一个或者多个密钥协商算法中,确定与第二节点进行密钥协商时所

使用的密钥协商算法。示例性地,可供选择的密钥协商算法有:SM2、ECDH(基于 curve25519 的椭圆曲线)、TBPEKE(基于 SM2 的椭圆曲线)、TBPEKE(基于 curve25519 的椭圆曲线)。

作为一种可能的方案,第一节点选择的密钥协商算法包含 TPPEKE 算法,即,TPPEKE 算法作为第一节点和第二节点之间的协商密钥的算法。TBPEKE 算法所使用的椭圆曲线包含以下椭圆曲线中的一项或者多项:SM2 定义的椭圆曲线、或 Curve25519 等。因此,TBPEKE 算法可以包含:使用 SM2 定义的椭圆曲线的 TBPEKE 算法、使用 Curve25519 的 TBPEKE 算法等。应理解,此处是为了方便描述使用不同椭圆曲线的 TBPEKE 算法所做的示例性的描述,具体实施过程中,还可以使用其他椭圆曲线,此处不一一列举。

可选的,当选定的密钥协商算法为 TBPEKE 算法时,至少一个公共参数包含:阶数为 p 的群(或群中的部分元素),和/或,群中的两个基点,如前述的第一基点和第二基点。该群与 TBPEKE 算法所使用的椭圆曲线相关。

在一种可能的设计中,第二节点在广播消息中携带其支持的密钥协商算法。其支持的密钥协商算法按照优先级顺序排列,优先级高的算法排在前面。第一节点根据第二节点的密钥协商算法能力,选择密钥协商算法。一些可能的设计中,第一节点选择的算法是第一节点和第二节点均支持的密钥协商算法,且在第二节点支持的密钥协商算法中优先级最高。

步骤 S602:第一节点生成第一私钥 SK_t 、计算公钥 PK_t ,其中,公钥 PK_t 作为第一密钥协商参数 KE_t 。

具体的,第一节点生成一个随机数作为私钥 SK_t ,其中 $1 \leq SK_t < p$ 。

第一节点基于 pw (第一口令)、 U 与 V (公共参数)计算 b (中间参数),其中:
 $b = (U + pw * V)$ 。第一节点根据 b 和私钥 SK_t 计算公钥 PK_t ,其中: $PK_t = SK_t * b$ 。

第一节点将公钥 PK_t 作为第一密钥协商参数 KE_t 。

步骤 S603:第一节点向第二节点发送关联请求消息。关联请求消息中携带 T 节点的 ID、算法的指示信息 KE_alg 、第一密钥协商参数 KE_t 和随机数 $NONCE_t$ 。

其中, KE_alg 用于指示第一节点选择的密钥协商算法。 $NONCE_t$ 为第一节点确定的一个随机数。

相应的,第二节点接收来自第一节点的关联请求消息。

步骤 S604:第二节点生成私钥 SK_g 、计算公钥 PK_g ,其中,公钥 PK_g 作为第二密钥协商参数 KE_g 。

具体的,第二节点生成一个随机数作为私钥 SK_g ,其中 $1 \leq SK_g < p$ 。

第二节点基于 pw (第一口令)、 U 与 V (公共参数)计算 b (中间参数),其中:
 $b = (U + pw * V)$ 。第二节点根据 b 和私钥 SK_g 计算公钥 PK_g ,其中: $PK_g = SK_g * b$ 。

第一节点将公钥 PK_g 作为第一密钥协商参数 KE_g 。

步骤 S605:第二节点根据私钥 SK_g 和第一密钥协商参数 KE_t 确定第一密钥 K_{KE} 。

具体的,第二节点通过如下方式得到第一密钥:第一密钥 $= SK_g * KE_t$ 。由于第一密钥协商参数 KE_t 满足如下式子: $KE_t = SK_t * (U + pw * V)$,因此,第一密钥 K_{KE} 可以满足如下式子:

$$K_{KE} = SK_g * KE_t = (SK_t * SK_g) * (U + pw * V)。$$

可选的,第二节点还可以基于第一密钥 K_{KE} 得到衍生的其他密钥。例如,第二节点根据第一密钥 K_{KE} 、随机数 $NONCE_t$ 和随机数 $NONCE_g$ 计算共享密钥 K_{gt} ,即:共享密钥 $K_{gt} = KDF(K_{KE}, NONCE_t, NONCE_g)$ 。

步骤 S606:第二节点基于 K_{KE} 和 PSK 计算第二认证信息 $AUTH_g$ 。

其中, PSK 为第二节点和第一节点之间的共享密钥, 可以根据口令等参数生成, 也可以预配置。

作为一种可能的方案, 第二认证信息通过如下方式计算得到: $AUTHg = AUF(PSK, K_{KE})$ 高 32 比特。

作为又一种可能的方案, 参与生成第二认证信息的可选参数还可以包括密钥 Kgt、PSK、第一新鲜参数、第二新鲜参数、关联请求消息、安全上下文请求消息中的一项或者多项。示例性的, 第二认证信息通过如下方式计算得到: $AUTHg = AUF(PSK, K_{KE}, NONCEg, \text{关联请求消息})$ 高 32 比特。

可选的, 第二节点还可以生成随机数 NONCEg。

步骤 S607: 第二节点向第一节点发送安全上下文请求消息。安全上下文请求消息中携带第二密钥协商参数 KEg、随机数 NONCEg、第二认证信息 AUTHg。

相应的, 第一节点接收来自第二节点的安全上下文请求消息。

步骤 S608: 第一节点根据私钥 SKt 和第二密钥协商参数 KEg 确定第二密钥 K_{KE} 。

具体的, 第一节点通过如下方式得到第二密钥: 第二密钥 = $SKt * KEg$ 。由于第二密钥协商参数 KEg 满足如下式子: $KEg = SKg * (U + pw * V)$, 因此, 第二密钥 K_{KE} 可以满足如下式子:

$$K_{KE} = SKt * KEg = (SKt * SKg) * (U + pw * V)。$$

由于第一密钥 $K_{KE} = (SKt * SKg) * (U + pw * V)$ = 第二密钥 K_{KE} , 因此第一节点和第二节点通过交换密钥协商参数得到了一致的密钥 K_{KE} 。

可选的, 第一节点还可以基于第二密钥 K_{KE} 得到衍生的其他密钥。例如, 第一节点根据第二密钥 K_{KE} 、随机数 NONCEt 和随机数 NONCEg 计算共享密钥 Kgt, 即: 共享密钥 $Kgt = KDF(K_{KE}, NONCEt, NONCEg)$ 。

步骤 S609: 第一节点基于 K_{KE} 和 PSK 计算第一认证信息 AUTHt。

其中, PSK 为第二节点和第一节点之间的共享密钥, 可以根据口令等参数生成, 也可以预配置。

作为一种可能的方案, 第一认证信息通过如下方式计算得到: $AUTHt = AUF(PSK, K_{KE})$ 高 32 比特。

作为又一种可能的方案, 参与生成第一认证信息的可选参数还可以包括密钥 Kgt、PSK、第一新鲜参数、第二新鲜参数、关联请求消息、安全上下文请求消息中的一项或者多项。示例性的, 第一认证信息通过如下方式计算得到:

$AUTHt = AUF(PSK, K_{KE}, \text{安全上下文请求消息}, NONCEt, \text{第二节点的密钥协商算法能力})$ 高 32 比特。

作为一种可能的方案, 第一节点验证第二认证信息 AUTHg 是否正确, 如果正确则第一节点生成第一认证信息 AUTHt。

可选的, 安全上下文请求消息包含完整性验证信息。第一节点验证安全上下文请求消息完整性和第二认证信息 AUTHg 通过, 则生成第一认证信息 AUTHt。

步骤 S610: 第一节点向第二节点发送安全上下文响应消息。安全上下文响应消息中携带第一认证信息 AUTHt。

相应的, 第二节点接收来自第一节点的安全上下文响应消息。

第二节点验证第一认证信息 AUTHt。如果正确则执行步骤 S611。

步骤 S611: 第二节点向第一节点发送关联建立消息。

作为一种可能的方案，安全上下文响应消息包含完整性验证信息。在第二节点验证安全上下文响应消息完整性和第一认证信息 AUTHt 通过的情况下，向第一节点发送关联建立消息。

在图 6 所示的实施例中，在第一节点请求接入第二节点时，第一节点可以选择基于椭圆曲线理论的 TBPEKE 算法来进行密钥协商，其密钥协商过程中选定的公共参数位于椭圆曲线上。由于椭圆曲线上的离散对数问题，通过安全参数和公共参数计算得到中间参数是较为容易的，但是，通过获取第一密钥协商参数和公共参数破解安全参数是困难的。因此，通过 TBPEKE 算法和公共参数，可以降低安全参数被破解的可能性，提升节点的安全性。

在攻击者请求接入第二节点时，由于没有一致的安全参数则不能生成一致的共享密钥，从而使得攻击者无法接入第二节点，因此可以避免攻击者接入第二节点，防止第二节点与身份不可信的攻击者关联成功。

请参见图 7，图 7 是本申请实施例提供的又一种可能的通信方法的流程图。进一步的，该方法可以基于图 2 所示的架构来实现。如图 7 所示的通信方法可以包括步骤 S701 至步骤 S717。应理解，本申请为了方便描述，故通过 S701 至 S717 这一顺序进行描述，并不旨在限定一定通过上述顺序进行执行。本申请实施例对于上述一个或多个步骤的执行的先后顺序、执行的时间、执行的次数等不做限定。S701 至步骤 S717 具体如下：

步骤 S701（可选）：第一节点选择密钥协商算法。

具体地，第一节点从一个或者多个密钥协商算法中，确定与第二节点进行密钥协商时所使用的密钥协商算法。示例性地，可供选择的密钥协商算法有：SM2、ECDH（基于 curve25519 的椭圆曲线）、TBPEKE（基于 SM2 的椭圆曲线）、TBPEKE（基于 curve25519 的椭圆曲线）。

作为一种可能的方案，第一节点选择的密钥协商算法包含 TPPEKE 算法，即，TPPEKE 算法作为第一节点和第二节点之间的协商密钥的算法。TBPEKE 算法所使用的椭圆曲线包含以下椭圆曲线中的一项或者多项：SM2 定义的椭圆曲线、或 Curve25519 等。因此，TBPEKE 算法可以包含：使用 SM2 定义的椭圆曲线的 TBPEKE 算法、使用 Curve25519 的 TBPEKE 算法等。应理解，此处是为了方便描述使用不同椭圆曲线的 TBPEKE 算法所做的示例性的描述，具体实施过程中，还可以使用其他椭圆曲线，此处不一一列举。

可选的，当选定的密钥协商算法为 TBPEKE 算法时，至少一个公共参数包含：阶数为 p 的群（或群中的部分元素），和/或，群中的两个基点，如前述的第一基点和第二基点。该群与 TBPEKE 算法所使用的椭圆曲线相关。

在一种可能的设计中，第二节点在广播消息中携带其支持的密钥协商算法。其支持的密钥协商算法按照优先级顺序排列，优先级高的算法排在前面。第一节点根据第二节点的密钥协商算法能力，选择密钥协商算法。一些可能的设计中，第一节点选择的算法是第一节点和第二节点均支持的密钥协商算法，且在第二节点支持的密钥协商算法中优先级最高。

步骤 S702：第一节点生成随机数 x ，计算 $X=x*U$ 。

可选的，步骤 S703 在密钥协商算法为 TPPEKE 算法的情况下执行。其中， U 为预先定义的基点。

可选的， U 属于阶数为 p （可选 p 为素数）的群，该群所对应的椭圆曲线为第一节点选定的密钥协商算法所使用的椭圆曲线。例如，当第一节点选择 TBPEKE（基于 SM2 的椭圆曲线）算法时， U 属于 SM2 的椭圆曲线相关的、阶数为 p 的群中的点（即：第二基点）。

可选的, 第一节点可以向第二节点发送选定的椭圆曲线的信息, 用于描述第一公共参数相关的椭圆曲线。

步骤 703 (可选): 第一节点向第二节点发送密钥协商算法的指示信息。相应的, 第二节点接收来自第一节点的密钥协商算法的指示信息。

例如, 通过 KEalg 来指示第一节点选择的密钥协商算法。

或者, 第一节点可以向第二节点发送自身支持的密钥协商算法, 相应的, 第二节点可以基于与第一节点相同的选择方式, 得到第一节点所选择的密钥协商算法。

步骤 S704: 第一节点向第二节点发送 X。相应的, 第二节点接收来自第一节点的 X。

可选的, 密钥协商算法的指示信息和 X 可以携带在同一条消息中, 也可以使用不同消息发送。

步骤 S705: 第二节点生成随机数 y、计算 $Y=y*U$ 、计算 $V=y*X$ 。

步骤 S706: 第二节点生成私钥 SKg、计算公钥 PKg, 其中, 公钥 PKg 作为第二密钥协商参数 KEg。

具体的, 第二节点生成一个随机数作为私钥 SKg, 其中 $1 \leq SKg < p$ 。

第二节点基于 pw (第一口令)、U 与 V (公共参数) 计算 b (中间参数), 其中: $b = (U + pw * V)$ 。第二节点根据 b 和私钥 SKg 计算公钥 PKg, 其中: $PKg = SKg * b$ 。

第一节点将公钥 PKg 作为第一密钥协商参数 KEg。

步骤 S707: 第二节点向第一节点发送 Y。相应的, 第一节点接收来自第二节点的 Y。

步骤 S708: 第一节点计算 $V=x*Y$ 。

步骤 S709: 生成私钥 SKt、计算公钥 PKt, 其中, 公钥 PKt 作为第一密钥协商参数 KEt。

具体的, 第一节点生成一个随机数作为私钥 SKt, 其中 $1 \leq SKt < p$ 。

第一节点基于 pw (第一口令)、U 与 V (公共参数) 计算 b (中间参数), 其中: $b = (U + pw * V)$ 。第一节点根据 b 和私钥 SKt 计算公钥 PKt, 其中: $PKt = SKt * b$ 。

第一节点将公钥 PKt 作为第一密钥协商参数 KEt。

步骤 S710: 第一节点向第二节点发送关联请求消息。关联请求消息中携带第一密钥协商参数 KEt、随机数 NONCEt、T 节点的 ID (可选) 和算法的指示信息 KE alg (可选)。

其中, NONCEt 为第一节点确定的一个随机数。

相应的, 第二节点接收来自第一节点的关联请求消息。

步骤 S711: 第二节点根据私钥 SKg 和第一密钥协商参数 KEt 确定第一密钥 K_{KE} 。

具体的, 第二节点通过如下方式得到第一密钥: 第一密钥 = $SKg * KEt$ 。由于第一密钥协商参数 KEt 满足如下式子: $KEt = SKt * (U + pw * V)$, 因此, 第一密钥 K_{KE} 可以满足如下式子:

$$K_{KE} = SKg * KEt = (SKt * SKg) * (U + pw * V)。$$

可选的, 第二节点还可以基于第一密钥 K_{KE} 得到衍生的其他密钥。例如, 第二节点根据第一密钥 K_{KE} 、随机数 NONCEt 和随机数 NONCEg 计算共享密钥 Kgt, 即: 共享密钥 $Kgt = KDF(K_{KE}, NONCEt, NONCEg)$ 。

可选的, 上述步骤 S706 可以在执行步骤 S711 时 (或之后) 执行。

步骤 S712: 第二节点基于 K_{KE} 和 PSK 计算第二认证信息 AUTHg。

其中, PSK 为第二节点和第一节点之间的共享密钥, 可以根据口令等参数生成, 也可以预配置。

作为一种可能的方案, 第二认证信息通过如下方式计算得到: $AUTHg = AUF (PSK, K_{KE})$ 高 32 比特。

作为又一种可能的方案,参与生成第二认证信息的可选参数还可以包括密钥 K_{gt} 、PSK、第一新鲜参数、第二新鲜参数、关联请求消息、安全上下文请求消息中的一项或者多项。示例性的,第二认证信息通过如下方式计算得到: $AUTH_g = AUF(PSK, K_{KE}, NONCE_g, \text{关联请求消息})|_{\text{高 32 比特}}$ 。

可选的,第二节点还可以生成随机数 $NONCE_g$ 。

步骤 S713: 第二节点向第一节点发送安全上下文请求消息。安全上下文请求消息中携带第二密钥协商参数 KE_g 、随机数 $NONCE_g$ 、第二认证信息 $AUTH_g$ 。

相应的,第一节点接收来自第二节点的安全上下文请求消息。

步骤 S714: 第一节点根据私钥 SK_t 和第二密钥协商参数 KE_g 确定第二密钥 K_{KE} 。

具体的,第一节点通过如下方式得到第二密钥: 第二密钥 = $SK_t * KE_g$ 。由于第二密钥协商参数 KE_g 满足如下式子: $KE_g = SK_g * (U + pw * V)$, 因此,第二密钥 K_{KE} 可以满足如下式子:

$$K_{KE} = SK_t * KE_g = (SK_t * SK_g) * (U + pw * V)。$$

由于第一密钥 $K_{KE} = (SK_t * SK_g) * (U + pw * V)$ = 第二密钥 K_{KE} , 因此第一节点和第二节点通过交换密钥协商参数得到了一致的密钥 K_{KE} 。

可选的,第一节点还可以基于第二密钥 K_{KE} 得到衍生的其他密钥。例如,第一节点根据第二密钥 K_{KE} 、随机数 $NONCE_t$ 和随机数 $NONCE_g$ 计算共享密钥 K_{gt} , 即: 共享密钥 $K_{gt} = KDF(K_{KE}, NONCE_t, NONCE_g)$ 。

步骤 S715: 第一节点基于 K_{KE} 和 PSK 计算第一认证信息 $AUTH_t$ 。

其中, PSK 为第二节点和第一节点之间的共享密钥,可以根据口令等参数生成,也可以预配置。

作为一种可能的方案,第一认证信息通过如下方式计算得到: $AUTH_t = AUF(PSK, K_{KE})|_{\text{高 32 比特}}$ 。

作为又一种可能的方案,参与生成第一认证信息的可选参数还可以包括密钥 K_{gt} 、PSK、第一新鲜参数、第二新鲜参数、关联请求消息、安全上下文请求消息中的一项或者多项。示例性的,第一认证信息通过如下方式计算得到:

$AUTH_t = AUF(PSK, K_{KE}, \text{安全上下文请求消息}, NONCE_t, \text{第二节点的密钥协商算法能力})|_{\text{高 32 比特}}$ 。

作为一种可能的方案,第一节点验证第二认证信息 $AUTH_g$ 是否正确,如果正确则第一节点生成第一认证信息 $AUTH_t$ 。

可选的,安全上下文请求消息包含完整性验证信息。第一节点验证安全上下文请求消息完整性和第二认证信息 $AUTH_g$ 通过,则生成第一认证信息 $AUTH_t$ 。

步骤 S716: 第一节点向第二节点发送安全上下文响应消息。安全上下文响应消息中携带第一认证信息 $AUTH_t$ 。

相应的,第二节点接收来自第一节点的安全上下文响应消息。

第二节点验证第一认证信息 $AUTH_t$ 。如果正确则执行步骤 S511。

步骤 S717(可选): 第二节点向第一节点发送关联建立消息。

作为一种可能的方案,安全上下文响应消息包含完整性验证信息。在第二节点验证安全上下文响应消息完整性和第一认证信息 $AUTH_t$ 通过的情况下,向第一节点发送关联建立消息。

在图 7 所示的实施例,第一节点和第二节点基于 TBPEKE 算法定义的椭圆曲线、通

过交换随机数得到公共参数 U、V。在第一节点请求接入第二节点时，第一节点可以选择基于椭圆曲线理论的 TBPEKE 算法来进行密钥协商，其密钥协商过程中使用 U、V 来参与生成密钥协商参数。由于椭圆曲线上的离散对数问题，通过安全参数和公共参数计算得到中间参数是较为容易的，但是，通过获取第一密钥协商参数和公共参数破解安全参数是困难的。因此，通过 TBPEKE 算法和公共参数，可以降低安全参数被破解的可能性，提升节点的安全性。

在攻击者请求接入第二节点时，由于没有一致的安全参数则不能生成一致的共享密钥，从而使得攻击者无法接入第二节点，因此可以避免攻击者接入第二节点，防止第二节点与身份不可信的攻击者关联成功。

上述图 6、图 7 所示实施例中，第一口令 pw 可以替换为 PSK。

上述详细阐述了本申请实施例的方法，下面提供本申请实施例的装置。

可以理解的是，本申请实施例提供的多个装置，例如通信装置，为了实现上述方法实施例中的功能，其包含了执行各个功能相应的硬件结构、软件单元、或硬件结构和软件结构的组合等。本领域技术人员应该很容易意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，本申请实施例能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以在不同的使用场景中，使用不同的装置实现方式来实现前述的方法实施例，对于装置的不同实现方式不应认为超出本申请实施例的范围。

本申请实施例可以对装置进行功能单元的划分。例如，可对应各个功能划分各个功能单元，也可将两个或两个以上的功能集成在一个功能单元中。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单元的形式实现。需要说明的是，本申请实施例中对单元的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

以下列举几种可能的装置。

上述详细阐述了本申请实施例的方法，下面提供了本申请实施例的装置。

请参见图 8，图 8 是本申请实施例提供的一种通信装置 80 的结构示意图。可选的，该通信装置 80 可以为独立设备，例如节点。或者，该通信装置 80 也可以独立设备（如节点）中的一个器件，例如芯片或者集成电路等。

该通信装置 80 可以包括接收单元 801、发送单元 802 和处理单元 803 中的一项或者多项。该通信装置 80 用于实现前述的通信方法，例如如图 4、图 6、或图 7 所示的通信方法。

在一种可能的设计中，通信装置 80 包含接收单元 801、发送单元 802 和处理单元 803，该通信装置 80 用于实现前述实施例中第二节点一侧的方法。

在一种可能的实施方式中，所述接收单元 801，用于接收来自第一节点的第一消息，所述第一消息包含第一密钥协商参数，所述第一密钥协商参数与第一私钥和中间参数相关联，所述中间参数与安全参数和至少一个公共参数相关联，所述安全参数为第一口令或所述第一节点与第二节点之间的预共享密钥 PSK，所述第一口令为所述第一节点与所述第二节点之间的约定接入口令；

所述发送单元 802，还用于向所述第一节点发送第二消息，所述第二消息包含第二密钥协商参数，所述第二密钥协商参数与第二私钥和所述中间参数相关联；

所述处理单元 803，用于根据所述第一密钥协商参数和所述第二私钥，得到第一密钥。

在又一种可能的实施方式中，所述接收单元 801，还用于接收来自所述第一节点的第三

消息,所述第三消息包含第一认证信息,所述第一认证信息与第二密钥相关联,所述第二密钥与所述第二密钥协商参数和所述第一私钥相关联;

所述处理单元 803,还用于根据第一密钥验证所述第一认证信息。

在又一种可能的实施方式中,所述第一密钥用于得到一个或者多个密钥。

作为一种可能的方案,第一密钥用于推演得到加密密钥、完整性密钥、或身份认证密钥等。

在又一种可能的实施方式中,所述发送单元 802,还用于:

如果所述第一认证信息验证通过,向所述第一节点发送关联建立消息。

在又一种可能的实施方式中,所述发送单元 802,还用于:

在所述第三消息的完整性和所述第一认证信息验证通过时,向所述第一节点发送关联建立消息。

在又一种可能的实施方式中,所述接收单元 801,还用于:

接收所述第一节点发送的密钥协商算法的指示信息,所述密钥协商算法包含 TBPEKE 算法。

可选的,所述密钥协商算法的指示信息包含第一密钥协商算法的指示信息,所述第一密钥协商算法的指示信息用于指示 TBPEKE 算法。

在又一种可能的实施方式中,所述至少一个公共参数包含:第一公共参数和第二公共参数;

其中,所述第一公共参数和所述第二公共参数与所述第一椭圆曲线相关,所述第一椭圆曲线为密钥协商算法对应的椭圆曲线,所述密钥协商算法包含所述 TBPEKE 算法。

在又一种可能的实施方式中,所述第一公共参数和所述第二公共参数属于所述第一椭圆曲线上的点。

在又一种可能的实施方式中,所述第一公共参数为预先定义的,所述第二公共参数通过所述第一公共参数、第一随机数和第二随机数确定,所述第一随机数来自所述第一节点,所述第二随机数来自所述第二节点。

在一种可能的实施方式中,所述至少一个公共参数包含至少一个基点,该至少一个基点属于阶数为 p 的群, p 为素数。

可选的,该群可以为关于在第一椭圆曲线上的运算的循环群或循环子群。

可选的,部分场景中基点也可以替换为生成元。

在又一种可能的实施方式中,当选定的密钥协商算法为 TBPEKE 算法时,至少一个公共参数包含:阶数为 p 的群中的部分或者全部元素, p 为素数。

其中,阶数为 p 的子群的基点(或称生成元)为 U 。对于选定的一个数 d , d 的取值范围是 $[1,p-1]$,则 dU 包含于该群中。

可选的,至少一个公共参数包含基点 U 。进一步可选的,至少一个公共参数还包含对 U 进行运算得到的 V , $V=dU$, d 的范围是 $[1,p-1]$ 。

在又一种可能的实施方式中,当选定的密钥协商算法为 TBPEKE 算法时,至少一个公共参数包含:阶数为 p 的群中的两个点。

可选的,这两个点可以是两个基点。或者可替换的,两个点中的一个为基点,另一个为根据基点计算得到的第二基点。为了便于描述,本申请统一称为第一基点和第二基点。

在又一种可能的实施方式中,当选定的密钥协商算法为 TBPEKE 算法时,TBPEKE 的公共参数包括:阶数为素数 p 的循环群,及群中的两个独立的基点 U 和 V 。

应理解,“独立的”是指U和V是两个取值不同的点,并不旨在限定U和V之间没有关联关系。

在又一种可能的实施方式中,所述接收单元801,还用于接收来自所述第一节点的第一计算值,所述第一计算值与第一随机数和第一公共参数相关,所述第一随机数由第一节点确定,所述第一公共参数为基于TBPEKE算法预先定义;

所述处理单元803,还用于根据第二随机数和所述第一计算值确定所述第二公共参数;

所述发送单元802,还用于向所述第一节点发送第二计算值,所述第二计算值与所述第二随机数和所述第一公共参数相关,所述第二计算值用于所述第一节点确定所述第二公共参数。

可选的,所述第一公共参数为前述的第一基点,所述第二公共参数为前述的第二基点。

在又一种可能的实施方式中,所述中间参数满足如下式子:

$$b = U + s * V,$$

其中,b为所述中间参数,U、V为所述至少一个公共参数,s为所述安全参数,*为椭圆曲线点乘运算,+为椭圆曲线点加运算。

在一种可能的实施方式中,U为第一基点,V为第二基点。进一步的,U、V属于阶数为p的群,p为素数。其中,该群相关的运算为在第一椭圆曲线上的运算。

第一椭圆曲线为选定的密钥协商算法所使用的椭圆曲线。示例性地,以选择的密钥协商算法是TBPEKE算法为例,第一椭圆曲线可以为:使用SM2定义的椭圆曲线、或Curve25519等。

在又一种可能的实施方式中,所述第一密钥协商参数KEt满足如下式子:

$$KEt = SKt * b,$$

所述第一密钥满足如下式子:

$$\text{第一密钥} = SKg * KEt = SKg * (SKt * b) = (SKt * SKg) * (U + s * V),$$

所述第二密钥协商参数KEg满足如下式子:

$$KEg = SKg * b,$$

所述第二密钥满足如下式子:

$$\text{第二密钥} = SKt * KEg = SKt * (SKg * b) = (SKt * SKg) * (U + s * V);$$

其中,SKt为所述第一私钥,SKg为所述第二私钥,“.”为乘法运算。

在又一种可能的实施方式中,所述第一私钥(SKt)的取值范围为[1, p),所述第二私钥(SKg)的取值范围为[1, p),其中,p为所述TBPEKE算法所使用的椭圆曲线的阶数。

在又一种可能的实施方式中,所述发送单元802,还用于:

广播所述第二节点的密钥协商算法能力,所述第二节点的密钥协商算法能力表征所述第二节点支持的密钥协商算法。

在又一种可能的实施方式中,所述第一节点支持的密钥协商算法按优先级顺序排列。

在又一种可能的实施方式中,所述第一消息还包括第一新鲜参数,所述第一消息还包括第一新鲜参数,所述第一认证信息与所述第一节点与所述第二节点之间的预共享密钥PSK、所述第二密钥、所述第二消息、所述第一新鲜参数和所述第二节点的密钥协商算法能力相关。

在又一种可能的实施方式中,所述处理单元803,还用于:

根据所述第一节点与所述第二节点之间的PSK、所述第一密钥、所述第二消息、所述第一新鲜参数和所述第二节点的密钥协商算法能力,验证所述第一认证信息。

在又一种可能的实施方式中，所述第二消息还包括第二认证信息和第二新鲜参数，所述处理单元，还用于：

通过所述第一节点与所述第二节点之间的 PSK、所述第一密钥、所述第二新鲜参数和所述第一消息，得到第二认证信息。

在又一种可能的实施方式中，所述第一消息还包含第一新鲜参数，所述第二消息中还包含第二新鲜参数；所述处理单元 803，还用于：

根据所述第一密钥、所述第一新鲜参数和所述第二新鲜参数得到第三密钥。

在又一种可能的实施方式中，所述 PSK 为预先配置、预先定义或者根据所述第一口令得到的。

在又一种可能的实施方式中，所述处理单元 803，还用于：

根据第一对应关系得到所述第一节点与所述第二节点之间的 PSK。

可以看出，第二节点可以通过对应关系的形式来存储 PSK 与第一节点的对应关系。因此，可以根据对应关系得到第一节点与第二节点之间的 PSK。

在又一种可能的实施方式中，所述处理单元，还用于：

根据所述第一口令、第一新鲜参数和第二新鲜参数确定所述第一节点与所述第二节点之间的 PSK。

在一种可能的设计中，PSK 是根据第一口令、第一密钥、第一新鲜参数和第二新鲜参数来确定的。

在一种可能的设计中，通信装置 80 包含接收单元 801 和发送单元 802，该通信装置 80 用于实现前述实施例中第一节点一侧的方法。

在一种可能的实施方式中，所述发送单元 802，用于向第二节点发送第一消息，所述第一消息包含第一密钥协商参数，所述第一密钥协商参数与第一私钥和中间参数相关联，所述中间参数与安全参数和至少一个公共参数相关联，所述安全参数为第一口令或第一节点与所述第二节点之间的预共享密钥 PSK，所述第一口令为所述第一节点与所述第二节点之间的约定接入口令；

所述接收单元 801，还用于接收来自所述第二节点的第二消息，所述第二消息包含第二密钥协商参数，所述第二密钥协商参数与第二私钥和所述中间参数相关联；

所述处理单元 803，用于根据所述第二密钥协商参数和所述第一私钥得到第二密钥。

在一种可能的实施方式中，所述发送单元 802，还用于向所述第一节点发送第三消息，所述第三消息包含所述第一认证信息，所述第一认证信息与第二密钥相关联。

在一种可能的实施方式中，所述第二密钥用于得到一个或者多个密钥。

作为一种可能的方案，第二密钥用于推演得到加密密钥、完整性密钥、或身份认证密钥等。

在又一种可能的实施方式中，所述接收单元 801，还用于：

接收来自所述第二节点的关联建立消息。

在又一种可能的实施方式中，所述通信装置还包含处理单元 803，所述处理单元 803 用于：

根据所述第二节点的密钥协商算法能力，选择第一密钥协商算法。其中，第二节点的密钥协商算法能力能够指示第二节点支持的一种或者多种密钥协商算法。

在又一种可能的实施方式中，所述发送单元 802，还用于向所述第二节点发送密钥协商

算法的指示信息,所述密钥协商算法的指示信息用于指示双基密码指数函数密钥交换 TBPEKE 算法。

可选的,由于使用的椭圆曲线不同,TBPEKE 算法的数量可以有多个。例如,TBPEKEe 包含以下椭圆曲线中的一项或者多项:SM2 定义的椭圆曲线、或 Curve25519 等。因此,TBPEKE 算法可以包含:使用 SM2 定义的椭圆曲线的 TBPEKE 算法、使用 Curve25519 的 TBPEKE 算法等。

在又一种可能的实施方式中,所述至少一个公共参数包含:第一公共参数和第二公共参数;

其中,所述第一公共参数和所述第二公共参数与所述第一椭圆曲线相关,所述第一椭圆曲线为密钥协商算法对应的椭圆曲线,所述密钥协商算法包含所述 TBPEKE 算法。

在又一种可能的实施方式中,所述第一公共参数和所述第二公共参数属于所述第一椭圆曲线上的点。

在又一种可能的实施方式中,所述第一公共参数为预先定义的,所述第二公共参数通过所述第一公共参数、第一随机数和第二随机数确定,所述第一随机数来自所述第一节点,所述第二随机数来自第二节点。

在一种可能的实施方式中,所述至少一个公共参数包含至少一个基点,该至少一个基点属于阶数为 p 的群, p 为素数。

可选的,该群可以为关于在第一椭圆曲线上的运算的循环群或循环子群。

可选的,部分场景中基点也可以替换为生成元。

在又一种可能的实施方式中,当选定的密钥协商算法为 TBPEKE 算法时,至少一个公共参数包含:阶数为 p 的群中的部分或者全部元素, p 为素数。

其中,阶数为 p 的子群的基点(或称生成元)为 U 。对于选定的一个数 d , d 的取值范围是 $[1,p-1]$,则 dU 包含于该群中。

可选的,至少一个公共参数包含基点 U 。进一步可选的,至少一个公共参数还包含对 U 进行运算得到的 V , $V=dU$, d 的范围是 $[1,p-1]$ 。

在又一种可能的实施方式中,当选定的密钥协商算法为 TBPEKE 算法时,至少一个公共参数包含:阶数为 p 的群中的两个点。

可选的,这两个点可以是两个基点。或者可替换的,两个点中的一个为基点,另一个为根据基点计算得到的第二基点。为了便于描述,本申请统一称为第一基点和第二基点。

在又一种可能的实施方式中,当选定的密钥协商算法为 TBPEKE 算法时,TBPEKE 的公共参数包括:阶数为素数 p 的循环群,及群中的两个独立的基点 U 和 V 。

应理解,“独立的”是指 U 和 V 是两个取值不同的点,并不旨在限定 U 和 V 之间没有关联关系。

在又一种可能的实施方式中,所述发送单元 802,还用于向所述第二节点发送第一计算值,所述第一计算值与第一随机数和第一公共参数相关,所述第一随机数由第一节点确定,所述第一公共参数为预先定义的;

所述接收单元 801,还用于接收来自所述第二节点的第二计算值,所述第二计算值与所述第二随机数和所述第一公共参数相关;

处理单元 803,用于根据第二随机数和所述第一计算值确定所述第二公共参数。

可选的,所述第一公共参数为前述的第一基点,所述第二公共参数为前述的第二基点。在又一种可能的实施方式中,所述中间参数满足如下式子:

$$b = U + s * V,$$

其中, b 为所述中间参数, U 、 V 为所述至少一个公共参数, s 为所述安全参数, “*” 为椭圆曲线点乘运算, “+” 为椭圆曲线点加运算。

在一种可能的实施方式中, U 为第一基点, V 为第二基点。进一步的, U 、 V 属于阶数为 p 的群, p 为素数。其中, 该群相关的运算为在第一椭圆曲线上的运算。

第一椭圆曲线为选定的密钥协商算法所使用的椭圆曲线。示例性地, 以选择的密钥协商算法是 TBPEKE 算法为例, 第一椭圆曲线可以为: 使用 SM2 定义的椭圆曲线、或 Curve25519 等。

在又一种可能的实施方式中, 所述第一密钥协商参数 KEt 满足如下式子:

$$KEt = SKt * b,$$

所述第一密钥满足如下式子:

$$\text{第一密钥} = SKg * KEt = SKg * (SKt * b) = (SKt * SKg) * (U + s * V),$$

所述第二密钥协商参数 KEg 满足如下式子:

$$KEg = SKg * b,$$

所述第二密钥满足如下式子:

$$\text{第二密钥} = SKt * KEg = SKt * (SKg * b) = (SKt * SKg) * (U + s * V);$$

其中, SKt 为所述第一私钥, SKg 为所述第二私钥, “.” 为乘法运算。

在又一种可能的实施方式中, 所述第一私钥 (SKt) 的取值范围为 $[1, p)$, 所述第二私钥 (SKg) 的取值范围为 $[1, p)$, 其中, p 为所述 TBPEKE 算法所使用的椭圆曲线的阶数。

在又一种可能的实施方式中, 所述接收单元 801, 还用于:

接收所述第二节点发送的所述第二节点的密钥协商算法能力, 所述第二节点的密钥协商算法能力表征所述第二节点支持的密钥协商算法。

在又一种可能的实施方式中, 所述第一节点支持的密钥协商算法按优先级顺序排列。

在又一种可能的实施方式中, 所述第一消息还包含第一新鲜参数, 所述第一消息还包括第一新鲜参数, 所述第一认证信息与所述第一节点与所述第二节点之间的预共享密钥 PSK 、所述第二密钥、所述第二消息、所述第一新鲜参数和所述第二节点的密钥协商算法能力相关联。

在又一种可能的实施方式中, 所述第二消息还包括第二认证信息和第二新鲜参数, 所述第二认证信息与所述第一节点与所述第二节点之间的 PSK 、所述第一密钥、所述第二新鲜参数和所述第一消息相关联。

在又一种可能的实施方式中, 所述处理单元 803 还用于:

根据所述第一节点与所述第二节点之间的 PSK 、所述第二密钥、所述第二新鲜参数和所述第一消息, 验证所述第二认证信息;

在所述第二消息的完整性和所述第二认证信息验证通过时, 生成所述第一认证信息。

在一种可能的实施方式中, 所述第一消息中还包含第一新鲜参数, 所述第二消息中还包含第二新鲜参数; 所述处理单元 803, 还用于:

根据所述第二密钥、所述第一新鲜参数和所述第二新鲜参数得到第四密钥。

在一种可能的实施方式中, 所述 PSK 为预先配置、预先定义或者根据所述第一口令得到的。

在又一种可能的实施方式中, 所述处理单元 803, 还用于:

根据第二对应关系得到所述第一节点与所述第二节点之间的 PSK 。

在又一种可能的实施方式中，所述处理单元 803，还用于：

根据所述第一指令、第一新鲜参数和第二新鲜参数确定所述第一节点与所述第二节点之间的 PSK。

请参见图 9，图 9 是本申请实施例提供的一种可能的通信装置 90 的结构示意图。

该通信装置 90 可以为车辆、无人机、机器人等独立设备，也可以为包含于独立设备中的器件，例如芯片、软件模块、或集成电路等。该通信装置 90 可以包括至少一个处理器 901 和通信接口 902。可选的，还可以包括至少一个存储器 903。进一步可选的，还可以包含连接线路 904，其中，处理器 901、通信接口 902 和/或存储器 903 通过连接线路 904 相连，通过连接线路 904 互相通信，传递控制和/或数据信号。可选的，通信装置 90 还可以包含感知模块、或输出模块等中的一项或者多项（图中未示出）。

其中：

(1) 处理器 901 是进行算术运算和/或逻辑运算的模块，具体可以包含以下装置中的一项或者多项：CPU、MCU、GPU、MPU、ASIC、FPGA、CPLD、协处理器（协助中央处理器完成相应处理和应用）、和/或 NPU 等。

(2) 通信接口 902 可以用于为所述至少一个处理器提供信息输入或者输出。在一些可能的场景中，通信接口 902 可以包含接口电路。和/或，所述通信接口 902 可以用于接收外部发送的数据和/或向外部发送数据。例如，通信接口 902 可以包括诸如以太网电缆等的有线链路接口，也可以是无线路径（Wi-Fi、蓝牙、通用无线传输、车载短距通信技术以及其他短距无线通信技术）接口。可选的，通信接口 902 还可以包括与接口耦合的发射器（如射频发射器、天线等），或者接收器等。

可选地，若通信装置 90 为独立设备时，通信接口 902 可以包括接收器和发送器。其中，接收器和发送器可以为相同的部件，或者为不同的部件。接收器和发送器为相同的部件时，可以将该部件称为收发器。

可选地，若通信装置 90 为芯片或电路时，通信接口 902 可以包括输入接口和输出接口，输入接口和输出接口可以是相同的接口，或者可以分别是不同的接口。

可选地，通信接口 902 的功能可以通过收发电路或收发的专用芯片实现。处理器 901 可以通过专用处理芯片、处理电路、处理器或通用芯片实现。

(3) 存储器 903 用于提供存储空间，存储空间中可以存储操作系统和计算机程序等数据。存储器 903 可以是随机存储记忆体（random access memory, RAM）、只读存储器（read-only memory, ROM）、可擦除可编程只读存储器（erasable programmable read only memory, EPROM）、或便携式只读存储器（compact disc read-only memory, CD-ROM）等等中的一种或者多种的组合。

其中，以上列举的通信装置 90 中各模块或单元的功能和动作仅为示例性说明。

通信装置 90 中各功能单元可用于实现前述的通信方法，例如如图 4、图 6 或图 7 所示的通信方法。这里为了避免赘述，省略其详细说明。

可选的，处理器 901，可以是专门用于执行前述方法的处理器（便于区别称为专用处理器），也可以是通过调用计算机程序来执行前述方法的处理器（便于区别称为专用处理器）。可选的，至少一个处理器还可以既包括专用处理器也包括通用处理器。

可选的，在通信装置 90 包括至少一个存储器 903 的情况下，若处理器 901 通过调用计算机程序来实现前述通信方法，该计算机程序可以存储在存储器 903 中。

本申请实施例还提供了一种芯片系统，该芯片系统包括处理器和通信接口，所述通信接口用于接收和/或发送数据，和/或，所述通信接口用于为所述处理器提供输入和/或输出。所述芯片系统用于实现前述的通信方法，例如图 4、图 6 或图 7 所述的方法。

本申请实施例还提供了一种计算机可读存储介质，所述计算机可读存储介质中存储有指令，当所述指令在至少一个处理器上运行时，实现前述的通信方法，例如图 4、图 6 或图 7 所述的方法。

本申请实施例还提供了一种计算机程序产品，该计算机程序产品包括计算机指令，所述计算机指令用于实现前述的通信方法，例如图 4、图 6 或图 7 所述的方法。

需要说明的是，本申请实施例中，“示例性的”或者“例如”等词用于表示作例子、例证或说明。本申请中被描述为“示例性的”或者“例如”的任何实施例或设计方案不应被解释为比其他实施例或设计方案更优选或更具优势。确切而言，使用“示例性的”或者“例如”等词旨在以具体方式呈现相关概念。

本申请中实施例提到的“至少一个”是指一个或者多个，“多个”是指两个或两个以上。“以下至少一项(个)”或其类似表达，是指的这些项中的任意组合，包括单项(个)或复数项(个)的任意组合。

例如，a、b、或 c 中的至少一项(个)，可以表示：a、b、c、(a 和 b)、(a 和 c)、(b 和 c)、或(a 和 b 和 c)，其中 a、b、c 可以是单个，也可以是多个。“和/或”，描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A、同时存在 A 和 B、单独存在 B 这三种情况，其中 A、B 可以是单数或者复数。字符“/”一般表示前后关联对象是一种“或”的关系。

以及，除非有相反的说明，本申请实施例使用“第一”、“第二”等序数词是用于对多个对象进行区分，不用于限定多个对象的顺序、时序、优先级或者重要程度。例如，第一设备和第二设备，只是为了便于描述，而并不是表示这第一设备和第二设备的结构、重要程度等的不同，在某些实施例中，第一设备和第二设备还可以是同样的设备。

上述实施例中所用，根据上下文，术语“当……时”可以被解释为意思是“如果……”或“在……后”或“响应于确定……”或“响应于检测到……”。以上所述仅为本申请的可选实施例，并不用以限制本申请，凡在本申请的构思和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也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，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

权利要求书

1.一种通信方法，其特征在于，所述方法包括：

接收来自第一节点的第一消息，所述第一消息包含第一密钥协商参数，所述第一密钥协商参数与第一私钥和中间参数相关联，所述中间参数与安全参数和至少一个公共参数相关联，所述安全参数为第一口令或所述第一节点与第二节点之间的预共享密钥 PSK，所述第一口令为所述第一节点与所述第二节点之间的约定接入口令；

向所述第一节点发送第二消息，所述第二消息包含第二密钥协商参数，所述第二密钥协商参数与第二私钥和所述中间参数相关联；

根据所述第一密钥协商参数和所述第二私钥得到第一密钥。

2.根据权利要求 1 所述的方法，其特征在于，所述第一密钥用于得到加密密钥、完整性密钥或身份认证密钥中的一项或者多项。

3.根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

接收来自所述第一节点的第三消息，所述第三消息包含第一认证信息，所述第一认证信息与第二密钥相关联，所述第二密钥与所述第二密钥协商参数和所述第一私钥相关联；

根据所述第一密钥验证所述第一认证信息。

4.根据权利要求 3 所述的方法，其特征在于，所述方法还包括：

在所述第三消息的完整性和所述第一认证信息验证通过时，向所述第一节点发送关联建立消息。

5.根据权利要求 1-4 任一项所述的方法，其特征在于，所述方法还包括：

接收所述第一节点发送的第一密钥协商算法的指示信息，所述第一密钥协商算法的指示信息用于指示双基密码指数函数密钥交换 TBPEKE 算法。

6.根据权利要求 1-5 任一项所述的方法，其特征在于，所述至少一个公共参数包含第一公共参数和第二公共参数；

其中，所述第一公共参数和所述第二公共参数与第一椭圆曲线相关，所述第一椭圆曲线为第一密钥协商算法对应的椭圆曲线，所述第一密钥协商算法为 TBPEKE 算法。

7.根据权利要求 6 所述的方法，其特征在于，所述方法还包括：

接收来自所述第一节点的第一计算值，所述第一计算值与第一随机数和第一公共参数相关，所述第一随机数由第一节点确定，所述第一公共参数为预先定义的；

根据第二随机数和所述第一计算值确定所述第二公共参数；

向所述第一节点发送第二计算值，所述第二计算值与所述第二随机数和所述第一公共参数相关。

8.根据权利要求 5-7 任一项所述的方法，其特征在于，所述中间参数满足如下式子：

$$b = U + s * V,$$

其中, b 为所述中间参数, U 、 V 为所述至少一个公共参数, s 为所述安全参数, $*$ 为椭圆曲线点乘运算, $+$ 为椭圆曲线点加运算。

9. 根据权利要求 5-8 任一项所述的方法, 其特征在于, 所述至少一个公共参数包含: 阶数为素数 p 的循环群, 及所述循环群中的两个独立的基点 U 和 V 。

10. 根据权利要求 8 或 9 所述的方法, 其特征在于, 所述第一密钥协商参数 KE_t 满足如下式子:

$$KE_t = SK_t * b,$$

所述第一密钥满足如下式子:

$$\text{第一密钥} = SK_g * KE_t,$$

所述第二密钥协商参数 KE_g 满足如下式子:

$$KE_g = SK_g * b,$$

所述第二密钥满足如下式子:

$$\text{第二密钥} = SK_t * KE_g;$$

其中, SK_t 为所述第一私钥, SK_g 为所述第二私钥。

11. 根据权利要求 5-10 任一项所述的方法, 其特征在于, 所述第一私钥的取值范围为 $[1, p)$, 所述第二私钥的取值范围为 $[1, p)$, 其中, p 为所述 TBPEKE 算法所使用的椭圆曲线的阶数。

12. 根据权利要求 1-11 任一项所述的方法, 其特征在于, 在所述接收来自第一节点的第一条消息之前, 所述方法还包括:

广播所述第二节点的密钥协商算法能力, 所述第二节点的密钥协商算法能力表征所述第二节点支持的密钥协商算法。

13. 根据权利要求 12 所述的方法, 其特征在于, 所述第二节点支持的密钥协商算法按优先级顺序排列。

14. 根据权利要求 3 或 4 所述的方法, 其特征在于, 所述第一消息还包括第一新鲜参数; 所述第一认证信息与所述 PSK、所述第二密钥、所述第二消息、所述第一新鲜参数和所述第二节点的密钥协商算法能力相关联;

所述根据所述第一密钥验证所述第一认证信息, 包括:

根据所述 PSK、所述第一密钥、所述第二消息、所述第一新鲜参数和所述第二节点的密钥协商算法能力, 验证所述第一认证信息。

15. 根据权利要求 1-14 任一项所述的方法, 其特征在于, 所述第二消息还包括第二认证信息和第二新鲜参数, 所述方法还包括:

通过所述 PSK、所述第一密钥、所述第二新鲜参数和所述第一消息, 得到所述第二认证信息。

16.一种通信方法，其特征在于，所述方法包括：

向第二节点发送第一消息，所述第一消息包含第一密钥协商参数，所述第一密钥协商参数与第一私钥和中间参数相关联，所述中间参数与安全参数和至少一个公共参数相关联，所述安全参数为第一口令或第一节点与所述第二节点之间的预共享密钥 PSK，所述第一口令为所述第一节点与所述第二节点之间的约定接入口令；

接收来自所述第二节点的第二消息，所述第二消息包含第二密钥协商参数，所述第二密钥协商参数与第二私钥和所述中间参数相关联；

根据所述第二密钥协商参数和所述第一私钥得到第二密钥。

17.根据权利要求 16 所述的方法，其特征在于，所述第二密钥用于得到加密密钥、完整性密钥或身份认证密钥中的一项或者多项。

18.根据权利要求 16 所述的方法，其特征在于，所述方法还包括：

向所述第一节点发送第三消息，所述第三消息包含第一认证信息，所述第一认证信息与所述第二密钥相关联。

19.根据权利要求 17 或 18 所述的方法，其特征在于，所述方法还包括：

接收来自所述第二节点的关联建立消息。

20.根据权利要求 16-19 任一项所述的方法，其特征在于，在向第二节点发送第一消息之前，所述方法还包括：

根据所述第二节点的密钥协商算法能力，选择第一密钥协商算法；

向所述第二节点发送第一密钥协商算法的指示信息，所述第一密钥协商算法的指示信息用于指示双基密码指数函数密钥交换 TBPEKE 算法。

21.根据权利要求 16-20 任一项所述的方法，其特征在于，所述至少一个公共参数包含第一公共参数和第二公共参数；

其中，所述第一公共参数和所述第二公共参数与所述第一椭圆曲线相关，所述第一椭圆曲线为第一密钥协商算法对应的椭圆曲线，所述第一密钥协商算法为 TBPEKE 算法。

22.根据权利要求 21 所述的方法，其特征在于，所述方法还包括：

向所述第二节点发送第一计算值，所述第一计算值与第一随机数和第一公共参数相关，所述第一随机数由第一节点确定，所述第一公共参数为预先定义的；

接收来自所述第二节点的第二计算值，所述第二计算值与第二随机数和所述第一公共参数相关；

根据所述第二随机数和所述第一计算值确定所述第二公共参数。

23.根据权利要求 20-22 任一项所述的方法，其特征在于，所述第一密钥协商算法为所述第一节点支持的密钥协商算法，且所述第一密钥协商算法在所述第二节点支持的密钥协商算法中优先级最高。

24.根据权利要求 20-23 任一项所述的方法,其特征在于,所述中间参数满足如下式子:

$$b = U + s * V,$$

其中, b 为所述中间参数, U 、 V 为所述至少一个公共参数, s 为所述安全参数*为椭圆曲线点乘运算, $+$ 为椭圆曲线点加运算。

25.根据权利要求 20-24 任一项所述的方法,其特征在于, U 为第一基点, V 为第二基点, U 、 V 属于阶数为 p 的循环群, p 为素数。

26.根据权利要求 24 或 25 所述的方法,其特征在于,所述第一密钥协商参数 KEt 满足如下式子:

$$KEt = SKt * b,$$

所述第一密钥满足如下式子:

$$\text{第一密钥} = SKg * KEt,$$

所述第二密钥协商参数 KEg 满足如下式子:

$$KEg = SKg * b,$$

所述第二密钥满足如下式子:

$$\text{第二密钥} = SKt * KEg;$$

其中, SKt 为所述第一私钥, SKg 为所述第二私钥。

27.根据权利要求 20-26 任一项所述的方法,其特征在于,所述第一私钥的取值范围为 $[1, p)$, 所述第二私钥的取值范围为 $[1, p)$, 其中, p 为所述 TBPEKE 算法所使用的椭圆曲线的阶数。

28.根据权利要求 16-27 任一项所述的方法,其特征在于,在向第二节点发送第一消息之前,所述方法还包括:

接收所述第二节点发送的所述第二节点的密钥协商算法能力,所述第二节点的密钥协商算法能力表征所述第二节点支持的密钥协商算法。

29.根据权利要求 28 所述的方法,其特征在于,所述第二节点支持的密钥协商算法按优先级顺序排列。

30.根据权利要求 16-29 任一项所述的方法,其特征在于,所述第一消息还包含第一新鲜参数,所述第一认证信息与所述 PSK、所述第二密钥、所述第二消息、所述第一新鲜参数和所述第二节点的密钥协商算法能力相关联。

31.根据权利要求 18 所述的方法,其特征在于,所述第二消息还包括第二认证信息和第二新鲜参数,所述第二认证信息与所述 PSK、所述第一密钥、所述第二新鲜参数和所述第一消息相关联;所述方法还包括:

根据所述 PSK、所述第二密钥、所述第二新鲜参数和所述第一消息,验证所述第二认证信息;

在所述第二消息的完整性和所述第二认证信息验证通过时,生成所述第一认证信息。

32.一种通信装置，其特征在于，包括：

接收单元，用于接收来自第一节点的第一消息，所述第一消息包含第一密钥协商参数，所述第一密钥协商参数与第一私钥和中间参数相关联，所述中间参数与安全参数和至少一个公共参数相关联，所述安全参数为第一口令或所述第一节点与第二节点之间的预共享密钥 PSK，所述第一口令为所述第一节点与所述第二节点之间的约定接入口令；

发送单元，还用于向所述第一节点发送第二消息，所述第二消息包含第二密钥协商参数，所述第二密钥协商参数与第二私钥和所述中间参数相关联；

处理单元，用于根据所述第一密钥协商参数和所述第二私钥得到第一密钥。

33.根据权利要求 32 所述的通信装置，其特征在于，所述第一密钥用于得到加密密钥、完整性密钥或身份认证密钥中的一项或者多项。

34.根据权利要求 32 所述的通信装置，其特征在于，

所述接收单元，还用于接收来自所述第一节点的第三消息，所述第三消息包含第一认证信息，所述第一认证信息与第二密钥相关联，所述第二密钥与所述第二密钥协商参数和所述第一私钥相关联；

处理单元，还用于根据第一密钥验证所述第一认证信息。

35.根据权利要求 32-34 任一项所述的通信装置，其特征在于，所述接收单元，还用于：

接收所述第一节点发送的第一密钥协商算法的指示信息，所述第一密钥协商算法的指示信息用于指示双基密码指数函数密钥交换 TBPEKE 算法。

36.一种通信装置，其特征在于，包括：

发送单元，用于向第二节点发送第一消息，所述第一消息包含第一密钥协商参数，所述第一密钥协商参数与第一私钥和中间参数相关联，所述中间参数与安全参数和至少一个公共参数相关联，所述安全参数为第一口令或第一节点与所述第二节点之间的预共享密钥 PSK，所述第一口令为所述第一节点与所述第二节点之间的约定接入口令；

接收单元，还用于接收来自所述第二节点的第二消息，所述第二消息包含第二密钥协商参数，所述第二密钥协商参数与第二私钥和所述中间参数相关联；

处理单元，用于根据所述第二密钥协商参数和所述第一私钥得到第二密钥。

37.根据权利要求 36 所述的通信装置，其特征在于，所述第二密钥用于得到加密密钥、完整性密钥或身份认证密钥中的一项或者多项。

38.根据权利要求 36 所述的通信装置，其特征在于，

所述发送单元，还用于向所述第一节点发送第三消息，所述第三消息包含所述第一认证信息，所述第一认证信息与第二密钥相关联。

39.根据权利要求 36-38 任一项所述的通信装置，其特征在于，所述通信装置还包括处理单元，

所述处理单元，用于根据所述第二节点的密钥协商算法能力，选择第一密钥协商算法；
所述发送单元，还用于向所述第二节点发送第一密钥协商算法的指示信息，所述第一密钥协商算法的指示信息用于指示双基密码指数函数密钥交换 TBPEKE 算法。

40. 一种芯片系统，其特征在于，所述芯片系统包括至少一个处理器和通信接口，所述通信接口用于发送和/或接收数据，所述至少一个处理器用于调用至少一个存储器中存储的计算机程序，使得所述芯片系统实现如权利要求 1-15 任一项所述的方法，或者实现如权利要求 16-31 任一项所述的方法。

41. 一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中存储有计算机程序，当所述计算机程序在计算机上运行时，使得所述计算机执行如权利要求 1-15 任一项所述的方法，或执行如权利要求 16-31 任一项所述的方法。

42. 一种通信系统，其特征在于，包括：

第二节点，所述第二节点包含如权利要求 32-35 任一项所述的通信装置；

第一节点，所述第一节点包含如权利要求 36-39 任一项所述的通信装置。

43. 一种车辆，其特征在于，所述车辆包含第一节点和/或第二节点，其中：

所述第二节点包含如权利要求 32-35 任一项所述的通信装置，或者，所述第二节点为实现如权利要求 1-15 任一项所述的方法的节点；

所述第一节点包含如权利要求 36-39 任一项所述的通信装置，或者，所述第一节点为实现如权利要求 16-31 任一项所述的方法的节点。

44. 一种通信系统，其特征在于，包括：实现如权利要求 1-15 任一项所述的方法的第二节点和实现如权利要求 16-31 任一项所述的方法的第一节点。