(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101807997 B
(45)授权公告日 2012.08.22

(21)申请号 201010162213.6
(22)申请日 2010.04.28
(73)专利权人 中国工商银行股份有限公司
地址 100140 北京市西城区复兴门内大街55号
(72)发明人 赵晖
(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 周国城
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 201656997 U,2010.11.24, 权利要求1-15.

审查员 刘静

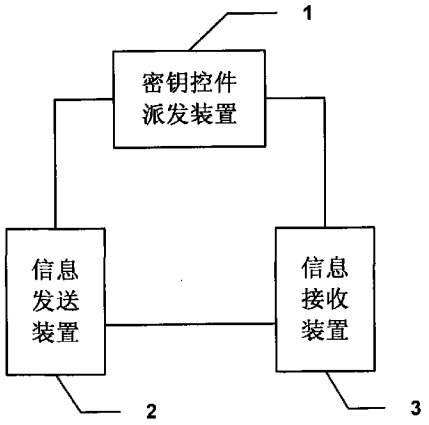
权利要求书 3 页 说明书 10 页 附图 4 页

(54)发明名称

一种生成传输密钥的装置及方法

(57)摘要

本发明公开了一种生成传输密钥的装置及方法。传输密钥是由通讯双方根据本方产生的私钥和对方传输过来的交互密钥，通过第三方派发的传输密钥生成算法共同生成，即使对方传输过来的交互密钥在网络中被截取也无法单独生成传输密钥，所述第三方派发的传输密钥生成算法使得双方使用的算法一致，并且在双方本地生成的传输密钥相等，从而达到对称加密算法的效果。双方的本地私钥通过随机生成，使用一次就失效，保证了传输密钥即使被窃取或破解也不会对下一次传输造成影响。传输密钥生成算法由第三方派发，对于通讯双方透明且一致，可以是每次重新派发，或者是定期、不定期派发，还可以是随机派发，进一步提升交互密钥和传输密钥的安全。



CN 101807997 B

1. 一种生成传输密钥的装置，其特征在于，该装置包括通过网络相互耦合连接的密钥控件派发装置 (1)、信息发送装置 (2) 和信息接收装置 (3)，其中：

密钥控件派发装置 (1)，是作为通讯双方的信息发送装置 (2) 和信息接收装置 (3) 的第三方，产生密钥控件和密钥控件信息，该密钥控件包含有交互密钥生成算法和传输密钥生成算法，将该密钥控件信息添加到该密钥控件，并发送给信息发送装置 (2) 和信息接收装置 (3)；

信息发送装置 (2) 和信息接收装置 (3)，均是一个 web 服务器，接收由密钥控件派发装置 (1) 发送的密钥控件，分别根据密钥控件中被添加的密钥控件信息对所接收的密钥控件进行认证，并分别利用密钥控件中的交互密钥生成算法生成各自的交互密钥，将该交互密钥与校验码、时间戳以及认证信息组成交互密钥信息包，然后将所述交互密钥信息包传输给对方，在分别收到对方的交互密钥信息包后，利用本地私钥和接收到的对方的交互密钥，通过调用密钥控件中的传输密钥生成算法生成各自的传输密钥，该两个传输密钥相等；最后，各自利用生成的传输密钥对需要传输的信息进行加解密。

2. 根据权利要求 1 所述的生成传输密钥的装置，其特征在于，所述密钥控件派发装置 (1) 包括相互连接的控件信息生成单元 (11) 和密钥控件生成单元 (12)，其中：

控件信息生成单元 (11)，产生密钥控件信息，该密钥控件信息至少包括安全控制 ID、版本号和控件使用期限；

密钥控件生成单元 (12)，抽用各种算法生成密钥控件，该密钥控件生成单元 (12) 包括交互密钥生成算法控件和传输密钥生成算法控件。

3. 根据权利要求 1 所述的生成传输密钥的装置，其特征在于，所述信息发送装置 (2) 或信息接收装置 (3) 均包括私钥生成单元 (201)、交互密钥生成单元 (202)、传输密钥生成单元 (203)、签名信息认证单元 (204)、校验码认证单元 (205)、时间戳校验单元 (206)、数据保存清理单元 (207)、信息发送单元 (208) 和主控单元 (209)，且私钥生成单元 (201)、交互密钥生成单元 (202)、传输密钥生成单元 (203)、签名信息认证单元 (204)、校验码认证单元 (205)、时间戳校验单元 (206)、数据保存清理单元 (207) 和信息发送单元 (208) 均连接于主控单元 (209)。

4. 根据权利要求 3 所述的生成传输密钥的装置，其特征在于，所述主控单元 (209) 接收来自密钥控件派发装置 (1) 的数据，并协调内部私钥生成单元 (201)、交互密钥生成单元 (202)、传输密钥生成单元 (203)、签名信息认证单元 (204)、校验码认证单元 (205)、时间戳校验单元 (206)、数据保存清理单元 (207) 和信息发送单元 (208) 完成密钥生成、交互以及认证工作。

5. 根据权利要求 3 所述的生成传输密钥的装置，其特征在于，所述私钥生成单元 (201) 生成本地私钥，并提供给主控单元 (209)，作为交互密钥生成单元的输入。

6. 根据权利要求 3 所述的生成传输密钥的装置，其特征在于，所述交互密钥生成单元 (202) 从主控单元 (209) 接收密钥控件派发装置 (1) 发送来的交互密钥生成控件 F(X)，将所述私钥生成单元 (201) 生成的本地私钥作为输入，生成交互密钥。

7. 根据权利要求 3 所述的生成传输密钥的装置，其特征在于，所述传输密钥生成单元 (203) 从主控单元 (209) 接收密钥控件派发装置 (1) 发送来的传输密钥生成控件 G(X, Y)，利用对方装置发送来的已生成的对方交互密钥和本地私钥信息，生成传输密钥。

8. 根据权利要求 3 所述的生成传输密钥的装置，其特征在于，所述签名信息认证单元 (204) 验证交互密钥信息包中的认证信息，密钥控件派发装置 (1) 在提供交互密钥生成算法控件和传输密钥生成算法控件这两种密钥生成控件时均加入了密钥控件信息，签名信息认证单元 (204) 使用公知的密钥控件派发装置的签名公钥对这两种加密后的密钥生成控件进行解密，只有来自合法密钥控件派发装置的密钥生成控件才可以解出正确明文，解出明文后首先验证身份 ID 是否正确，然后判断当前日期是否在控件有效范围内，最后获取版本信息用作后续交互确认控件一致性。

9. 根据权利要求 8 所述的生成传输密钥的装置，其特征在于，所述签名信息认证单元 (204) 进一步在向对方装置发送交互密钥前，先使用自身的签名私钥对交互密钥信息包进行加密，在接收到对方的交互密钥信息包之后才能使用公知的对方签名公钥解密交互密钥信息包，然后交由主控单元 (209) 分发处理。

10. 根据权利要求 3 所述的生成传输密钥的装置，其特征在于，所述校验码认证单元 (205) 调用自身包含的某种校验码算法对已生成的交互密钥信息包增加检验码信息，以保证形成更安全的交互密钥信息包，其中校验码认证单元 (205) 包含有多种校验码算法，该校验码算法至少是 CRC 校验算法或奇偶校验算法。

11. 根据权利要求 10 所述的生成传输密钥的装置，其特征在于，所述校验码认证单元 (205) 进一步从主控单元 (209) 接收对方装置发送来的交互密钥信息包，并对其校验码进行验证。

12. 根据权利要求 3 所述的生成传输密钥的装置，其特征在于，所述时间戳校验单元 (206) 认证交互密钥信息包是否已经失效，并根据包内时间戳信息与各自系统的本地时间进行比较，判断是否超时以防止简单的重放攻击。

13. 根据权利要求 3 所述的生成传输密钥的装置，其特征在于，所述数据保存清理单元 (207) 保存密钥交互期间的临时数据，并在交互结束后执行数据清理工作。

14. 根据权利要求 13 所述的生成传输密钥的装置，其特征在于，所述数据保存清理单元 (207) 还包括一个对称加密模块，所述主控单元 (209) 将临时数据存入数据保存清理单元 (207) 之前，首先通过该对称加密模块调用主控单元 (209) 的签名密钥对临时数据进行加密，以密文模式放入数据保存清理单元进行安全的存储；当其他单元需要调用临时数据时，所述主控单元 (209) 先通过该对称加密模块解密密文，从而获取明文信息，并交付其他单元使用。

15. 根据权利要求 3 所述的生成传输密钥的装置，其特征在于，所述信息发送单元 (208) 从主控单元 (209) 获取待发送的交互密钥信息包。

16. 一种生成传输密钥的方法，应用于权利要求 1 所述的传输密钥生成装置，其特征在于，该方法包括：

密钥控件派发装置 (1) 产生密钥控件和密钥控件信息，将该密钥控件信息添加到该密钥控件，并将形成的密钥控件发送给信息发送装置 (2) 和信息接收装置 (3)；

信息发送装置 (2) 和信息接收装置 (3) 接收该密钥控件，分别根据密钥控件中被添加的密钥控件信息对所接收的密钥控件进行认证；

信息发送装置 (2) 和信息接收装置 (3) 分别生成各自的交互密钥，将该交互密钥与校验码、时间戳以及认证信息组成交互密钥信息包，然后将该交互密钥信息包传输给对方；

在信息发送装置 (2) 和信息接收装置 (3) 分别收到对方的交互密钥信息包后，利用本地私钥和接收到的对方的交互密钥，通过调用交互密钥信息包中密钥控件包含的传输密钥生成算法生成各自的传输密钥，该两个传输密钥相等。

17. 根据权利要求 16 所述生成传输密钥的方法，其特征在于，所述密钥控件派发装置 (1) 产生密钥控件和密钥控件信息，将该密钥控件信息添加到该密钥控件，包括 ：

密钥控件派发装置 (1) 产生密钥控件和密钥控件信息，该密钥控件包含有交互密钥生成算法和传输密钥生成算法，将该密钥控件信息添加到该密钥控件中的交互密钥生成算法和传输密钥生成算法，并使用签名私钥对添加了密钥控件信息的交互密钥生成算法和传输密钥生成算法进行加密。

18. 根据权利要求 16 所述生成传输密钥的方法，其特征在于，所述信息发送装置 (2) 和信息接收装置 (3) 分别生成各自的交互密钥，将该交互密钥与校验码、时间戳以及认证信息组成交互密钥信息包，包括 ：

信息发送装置 (2) 和信息接收装置 (3) 分别在本地生成私钥，并分别利用密钥控件中的交互密钥生成算法生成各自的交互密钥，然后将该交互密钥与校验码、时间戳以及认证信息组成交互密钥信息包。

19. 根据权利要求 16 所述生成传输密钥的方法，其特征在于，该方法在生成各自的传输密钥后还包括 ：

信息发送装置 (2) 和信息接收装置 (3) 各自利用生成的传输密钥对需要传输的信息进行加解密。

一种生成传输密钥的装置及方法

技术领域

[0001] 本发明涉及网络安全技术领域，尤其涉及一种生成传输密钥的装置及方法，生成的传输密钥配合对称加密算法，可以实现安全的加密数据传输。

背景技术

[0002] 高涉密级行业经常涉及大量的私密信息传输场景，需要使用安全传输协议和安全网络环境。在使用安全传输协议和安全网络环境的同时，目前广泛应用的是对称密码加密方法来传输私密信息，比如 3DES 等。

[0003] 在使用对称加密方法时，生成传输密钥的算法是实现的核心；而如何生成与保存传输密钥则是加密方法安全强度和实现性能的根本保证。一个好的密钥实现方案，应该具备以下特点：保证传输过程中密钥完全保密，能够便捷的及时更新密钥，能够抵御常见的攻击方法等。

[0004] 目前的大多密钥传输系统，采用了各种各样的安全传输算法和通讯通道以及协商机制，但是都基于一个共同点：需要事先产生一个密钥，同时此密钥需要保存在双方服务器一定长的时间用于后续应用。一旦在这段时间内被攻击者获取到密钥，后续通讯内容就完全暴露了，所以，为了避免这种风险，大多数密钥传输系统都要求周期更换密钥以尽可能的减少暴露后带来的损失。但是这种做法必定不能完全规避风险，而且更换一次密钥需要重新生成、协商以及传输过程，太过频繁会很大程度的提高实现成本。

发明内容

[0005] （一）要解决的技术问题

[0006] 有鉴于此，本发明的主要目的在于提供一种生成传输密钥的装置及方法，以提高传输密钥的安全性，降低基于对称加密算法传输系统的密钥被破解或窃取的风险。

[0007] （二）技术方案

[0008] 为达到上述目的，本发明提供了一种生成传输密钥的装置，该装置包括通过网络相互耦合连接的密钥控件派发装置 1、信息发送装置 2 和信息接收装置 3，其中：

[0009] 密钥控件派发装置 1，是作为通讯双方的信息发送装置 2 和信息接收装置 3 的第三方，产生密钥控件和密钥控件信息，该密钥控件包含有交互密钥生成算法和传输密钥生成算法，将该密钥控件信息添加到该密钥控件，并发送给信息发送装置 2 和信息接收装置 3；

[0010] 信息发送装置 2 和信息接收装置 3，均是一个 web 服务器，接收由密钥控件派发装置 1 发送的密钥控件，分别根据密钥控件中被添加的密钥控件信息对所接收的密钥控件进行认证，并分别利用密钥控件中的交互密钥生成算法生成控件生成各自的交互密钥，将该交互密钥与校验码、时间戳以及认证信息组成交互密钥信息包，然后将所述交互密钥信息包传输给对方，在分别收到对方的交互密钥信息包后，利用本地私钥和接收到的对方的交互密钥，通过调用密钥控件中的传输密钥生成算法生成各自的传输密钥，该两个传输密钥相等；最后，各自利用生成的传输密钥对需要传输的信息进行加解密。

[0011] 上述方案中，所述密钥控件派发装置 1 包括相互连接的控件信息生成单元 11 和密钥控件生成单元 12，其中：

[0012] 控件信息生成单元 11，产生密钥控件信息，该密钥控件信息至少包括安全控制 ID、版本号和控件使用期限；

[0013] 密钥控件生成单元 12，抽用各种算法生成密钥控件，该密钥控件生成单元 12 包括交互密钥生成算法控件和传输密钥生成算法控件。

[0014] 上述方案中，所述信息发送装置 2 或信息接收装置 3 均包括私钥生成单元 201、交互密钥生成单元 202、传输密钥生成单元 203、签名信息认证单元 204、校验码认证单元 205、时间戳校验单元 206、数据保存清理单元 207、信息发送单元 208 和主控单元 209，且私钥生成单元 201、交互密钥生成单元 202、传输密钥生成单元 203、签名信息认证单元 204、校验码认证单元 205、时间戳校验单元 206、数据保存清理单元 207 和信息发送单元 208 均连接于主控单元 209。

[0015] 上述方案中，所述主控单元 209 接收来自密钥控件派发装置 1 的数据，并协调内部私钥生成单元 201、交互密钥生成单元 202、传输密钥生成单元 203、签名信息认证单元 204、校验码认证单元 205、时间戳校验单元 206、数据保存清理单元 207 和信息发送单元 208 完成密钥生成、交互以及认证工作。

[0016] 上述方案中，所述私钥生成单元 201 生成本地私钥，并提供给主控单元 209，作为交互密钥生成单元的输入。

[0017] 上述方案中，所述交互密钥生成单元 202 从主控单元 209 接收密钥控件派发装置 1 发送来的交互密钥生成控件 F(X)，将所述私钥生成单元 201 生成的本地私钥作为输入，生成交互密钥。

[0018] 上述方案中，所述传输密钥生成单元 203 从主控单元 209 接收密钥控件派发装置 1 发送来的传输密钥生成控件 G(X, Y)，利用对方装置发送来的已生成的对方交互密钥和本地私钥信息，生成传输密钥。

[0019] 上述方案中，所述签名信息认证单元 204 验证交互密钥信息包中的认证信息，密钥控件派发装置 1 在提供交互密钥生成算法控件和传输密钥生成算法控件这两种密钥生成控件时均加入了密钥控件信息，签名信息认证单元 204 使用公知的密钥控件派发装置的签名公钥对这两种加密后的密钥生成控件进行解密，只有来自合法密钥控件派发装置的密钥生成控件才可以解出正确明文，解出明文后首先验证身份 ID 是否正确，然后判断当前日期是否在控件有效范围内，最后获取版本信息用作后续交互确认控件一致性。

[0020] 上述方案中，所述签名信息认证单元 204 进一步在向对方装置发送交互密钥前，先使用自身的签名私钥对交互密钥信息包进行加密，在接收到对方的交互密钥信息包之后才能使用公知的对方签名公钥解密交互密钥信息包，然后交由主控单元 209 分发处理。

[0021] 上述方案中，所述校验码认证单元 205 调用自身包含的某种校验码算法对已生成的交互密钥信息包增加检验码信息，以保证形成更安全的交互密钥信息包，其中校验码认证单元 205 包含有多种校验码算法，该校验码算法至少是 CRC 校验算法或奇偶校验算法。

[0022] 上述方案中，所述校验码认证单元 205 进一步从主控单元 209 接收对方装置发送来的交互密钥信息包，并对其校验码进行验证。

[0023] 上述方案中，所述时间戳校验单元 206 认证交互密钥信息包是否已经失效，并根

据包内时间戳信息与各自系统的本地时间进行比较，判断是否超时以防止简单的重放攻击。

[0024] 上述方案中，所述数据保存清理单元 207 保存密钥交互期间的临时数据，并在交互结束后执行数据清理工作。

[0025] 上述方案中，所述数据保存清理单元 207 还包括一个对称加密模块，所述主控单元 209 将临时数据存入数据保存清理单元 207 之前，首先通过该对称加密模块调用主控单元 209 的签名密钥对临时数据进行加密，以密文模式放入数据保存清理单元进行安全的存储；当其他单元需要调用临时数据时，所述主控单元 209 先通过该对称加密模块解密密文，从而获取明文信息，并交付其他单元使用。

[0026] 上述方案中，所述信息发送单元 208 从主控单元 209 获取待发送的交互密钥信息包。

[0027] 为达到上述目的，本发明还提供了一种生成传输密钥的方法，该方法包括：

[0028] 密钥控件派发装置 1 产生密钥控件和密钥控件信息，将该密钥控件信息添加到该密钥控件，并将形成的密钥控件发送给信息发送装置 2 和信息接收装置 3；

[0029] 信息发送装置 2 和信息接收装置 3 接收该密钥控件，分别根据密钥控件中被添加的密钥控件信息对所接收的密钥控件进行认证；

[0030] 信息发送装置 2 和信息接收装置 3 分别生成各自的交互密钥，将该交互密钥与校验码、时间戳以及认证信息组成交互密钥信息包，然后将该交互密钥信息包传输给对方；

[0031] 在信息发送装置 2 和信息接收装置 3 分别收到对方的交互密钥信息包后，利用本地私钥和接收到的对方的交互密钥，通过调用交互密钥信息包中密钥控件包含的传输密钥生成算法生成各自的传输密钥，该两个传输密钥相等。

[0032] 上述方案中，所述密钥控件派发装置 1 产生密钥控件和密钥控件信息，将该密钥控件信息添加到该密钥控件，包括：密钥控件派发装置 1 产生密钥控件和密钥控件信息，该密钥控件包含有交互密钥生成算法和传输密钥生成算法，将该密钥控件信息添加到该密钥控件中的交互密钥生成算法和传输密钥生成算法，并使用签名私钥对添加了密钥控件信息的交互密钥生成算法和传输密钥生成算法进行加密。

[0033] 上述方案中，所述信息发送装置 2 和信息接收装置 3 分别生成各自的交互密钥，将该交互密钥与校验码、时间戳以及认证信息组成交互密钥信息包，包括：信息发送装置 2 和信息接收装置 3 分别在本地生成私钥，并分别利用密钥控件中的交互密钥生成算法生成各自的交互密钥，然后将该交互密钥与校验码、时间戳以及认证信息组成交互密钥信息包。

[0034] 上述方案中，该方法在生成各自的传输密钥后还包括：信息发送装置 2 和信息接收装置 3 各自利用生成的传输密钥对需要传输的信息进行加解密。

[0035] （三）有益效果

[0036] 从上述技术方案可以看出，本发明提供的这种生成传输密钥的装置及方法，可以广泛用于使用对称密钥加密算法交互细密信息的应用场景，实现安全的密钥交互，其优点体现在如下方面：

[0037] 1、防截取攻击：在交互信道，即使攻击者截获了交互密钥 K_a 和 K_b，但是，因为各自的随机密钥 a，b 是不再网络中通讯的，攻击者无法获取。同时进一步保证 F(X) = Y 算法是不可逆的，则 a 和 b 也无法通过计算获得，可以保证传输密钥 K 的安全。

[0038] 2、密钥更换：由于双方的随机密钥a和b都是每次交互前随机生成的，也就使得实际的交互密钥或者传输密钥每次也都是随机变化的，从而避免了密钥长时间使用带来的泄漏风险。

[0039] 3、防重放，防阻塞：通过将交互密钥组成信息包，添加校验码和时间戳可以起到防重放防阻塞的作用。

附图说明

[0040] 图1是本发明提供的生成传输密钥装置的结构示意图；

[0041] 图2是密钥控件派发装置的结构示意图；

[0042] 图3是信息发送装置和信息接收装置的结构示意图；

[0043] 图4是依照本发明第一个实施例生成传输密钥的方法流程图；

[0044] 图5是依照本发明第二个实施例生成传输密钥的方法流程图；

[0045] 图6是交互密钥信息包的结构示意图。

具体实施方式

[0046] 为使本发明的目的、技术方案和优点更加清楚明白，以下结合具体实施例，并参照附图，对本发明进一步详细说明。

[0047] 本发明的技术核心是，传输密钥是由通讯双方根据本方产生的私钥和对方传输过来的交互密钥，通过第三方派发的传输密钥生成算法共同生成，即使对方传输过来的交互密钥在网络中被截取也无法单独生成传输密钥，所述第三方派发的传输密钥生成算法使得双方使用的算法一致，并且在双方本地生成的传输密钥相等，从而达到对称加密算法的效果。双方的本地私钥通过随机生成，使用一次就失效，保证了传输密钥即使被窃取或破解也不会对下一次传输造成影响。传输密钥生成算法由第三方派发，对于通讯双方透明且一致，可以是每次重新派发，或者是定期、不定期派发，还可以是随机派发，进一步提升交互密钥和传输密钥的安全。

[0048] 图1是本发明提供的生成传输密钥装置的结构示意图，该装置包含密钥控件派发装置1、信息发送装置2和信息接收装置3，且密钥控件派发装置1、信息发送装置2和信息接收装置3通过网络相互耦合连接。

[0049] 所述密钥控件派发装置1是通讯双方公认的第三方，可以是一个PC服务器或主机，用于产生密钥控件和密钥控件信息（密钥控件包括交互密钥生成算法控件和传输密钥生成算法控件，密钥控件信息包括安全控制ID、版本号和控件使用期限等），将该密钥控件信息添加到该密钥控件，形成包含有交互密钥生成算法以及传输密钥生成算法的密钥控件，然后发送给信息发送装置2和信息接收装置3。

[0050] 如图2所示，图2是密钥控件派发装置的结构示意图。密钥控件派发装置1包括控件信息生成单元11和密钥控件生成单元12。所述控件信息生成单元11用于产生密钥控件信息，该密钥控件信息包括安全控制ID、版本号和控件使用期限等。所述密钥控件生成单元12，用于抽用各种算法生成密钥控件，该密钥控件包括交互密钥生成算法控件和传输密钥生成算法控件。

[0051] 所述信息发送装置2和信息接收装置3，均可以是一个web服务器，用于接收由密

钥控件派发装置 1 发送的密钥控件，分别根据密钥控件中被添加的控件信息对所接收的密钥控件进行认证，并分别利用密钥控件中的交互密钥生成算法生成各自的交互密钥，再使用校验码、时间戳以及认证信息组成交互密钥信息包，以保证所交互的密钥信息的完整性和准确性，然后将所述交互密钥信息包传输给对方。所述交互密钥信息包组成见图 6。

[0052] 信息发送装置 2 和信息接收装置 3 在分别收到对方的交互密钥信息包后，对信息包数据合法性进行认证，认证通过后利用本地私钥和接收到的对方的交互密钥，通过调用传输密钥生成控件中的传输密钥生成算法生成各自的传输密钥，该两个传输密钥相等。最后，信息发送装置 2 和信息发送装置 3 利用生成的传输密钥对需要传输的信息进行加解密。

[0053] 图 3 是信息发送装置和信息接收装置的结构示意图，信息发送装置 2 和信息接收装置 3 均包含私钥生成单元 201、交互密钥生成单元 202、传输密钥生成单元 203、签名信息认证单元 204、校验码认证单元 205、时间戳校验单元 206、数据保存清理单元 207、信息发送单元 208 和主控单元 209。

[0054] 所述主控单元 209 用于接收来自密钥控件派发装置 1 的数据，并协调内部各功能单元完成密钥生成、交互以及认证等工作。

[0055] 所述私钥生成单元 201，用于生成本地私钥，并提供给主控单元 209，作为交互密钥生成单元的输入。例如，该单元内部在符合密钥强度的数值区间中可随机产生一个密钥数值，即私钥，并提供给主控单元 209，同时将这个私钥加入作废列表，后续不再使用，且作废列表定期清空。

[0056] 所述交互密钥生成单元 202 ：负责从主控单元 209 接收密钥控件派发装置 1 发送来的交互密钥生成控件 F(X)，将上述私钥生成单元 201 生成的本地私钥作为输入，生成交互密钥。

[0057] 所述传输密钥生成单元 203 ：负责从主控单元 209 接收密钥控件派发装置 1 发送来的传输密钥生成控件 G(X,Y)，利用对方装置发送来的已生成的对方交互密钥和本地私钥信息，从而生成传输密钥。

[0058] 所述签名信息认证单元 204 ：用于验证交互信息中的认证信息，密钥控件派发装置 1 在提供两种密钥生成控件时，均加入了密钥控件信息，签名信息认证单元 204 使用公知的密钥控件派发装置的签名公钥对两种加密后的密钥生成控件进行解密，只有来自合法密钥控件派发装置的控件才可以解出正确明文，解出明文后首先验证身份 ID 是否正确，然后判断当前日期是否在控件有效范围内，最后获取版本信息用作后续交互确认控件一致性。

[0059] 同时，所述签名信息认证单元 204 还负责在向对方装置发送交互密钥前，先使用自身的签名私钥对交互密钥信息包进行加密，从而在接收到对方的交互密钥信息包之后才能使用公知的对方签名公钥解密交互密钥信息包，然后交由主控单元 209 分发处理。

[0060] 所述校验码认证单元 205 ：包含有多种校验码算法，所述校验码算法可以是 CRC 校验算法，奇偶校验算法等。该单元负责调用某种校验码算法对已生成的交互密钥信息包增加检验码信息以保证形成更安全的交互密钥信息包 ；进一步，所述校验码认证单元 205 还负责从主控单元 209 接收对方装置发送来的交互密钥信息包，并对其校验码进行验证。

[0061] 所述时间戳校验单元 206 ：用于认证交互密钥信息包是否已经失效，并根据包内时间戳信息与各自系统的本地时间进行比较，判断是否超时以防止重放攻击。

[0062] 所述数据保存清理单元 207 ：用于保存密钥交互期间的临时数据以及进行交互结

束后的数据清理工作；进一步，数据保存清理单元 207 还可以增加一个简单的对称加密模块，主控单元 209 将临时数据存入本单元之前，首先通过所述对称加密模块调用主控单元的签名密钥将临时数据进行加密，以密文模式放入数据保存清理单元进行安全的存储；当其他单元需要调用临时数据时，主控单元 209 需要先通过此对称加密模块解密密文，从而获取明文信息，才能交付其他单元使用。此装置可以保证每次使用的私钥、交互密钥以及传输密钥的安全性，防止在应用过程中被窃取。

[0063] 所述信息发送单元 208：用于从主控单元 209 获取待发送的交互密钥信息包。

[0064] 基于图 1 至图 3 所示的生成传输密钥的装置，本发明还提供了一种生成传输密钥的方法，该方法包括以下步骤：

[0065] 步骤 1：密钥控件派发装置 1 产生密钥控件和密钥控件信息，将该密钥控件信息添加到该密钥控件，并将形成的密钥控件发送给信息发送装置 2 和信息接收装置 3；

[0066] 步骤 2：信息发送装置 2 和信息接收装置 3 接收该密钥控件，分别根据密钥控件中被添加的控件信息对所接收的密钥控件进行认证；

[0067] 步骤 3：信息发送装置 2 和信息接收装置 3 分别生成各自的交互密钥，再使用校验码、时间戳以及认证信息组成交互密钥信息包，然后将该交互密钥信息包传输给对方；

[0068] 步骤 4：在信息发送装置 2 和信息接收装置 3 分别收到对方的交互密钥信息包后，利用本地私钥和接收到的对方的交互密钥，通过调用传输密钥生成控件中的传输密钥生成算法生成各自的传输密钥，该两个传输密钥相等。

[0069] 其中，步骤 1 中所述密钥控件派发装置 1 产生密钥控件和密钥控件信息，并对产生的密钥控件进行加密，包括：密钥控件派发装置 1 产生密钥控件和密钥控件信息，该密钥控件包含有交互密钥生成算法和传输密钥生成算法，将该密钥控件信息添加到该密钥控件，并使用签名私钥对添加了密钥控件信息的交互密钥生成算法和传输密钥生成算法进行加密。

[0070] 步骤 3 中所述信息发送装置 2 和信息接收装置 3 分别生成各自的交互密钥，再使用校验码、时间戳以及认证信息组成交互密钥信息包，包括：信息发送装置 2 和信息接收装置 3 分别在本地生成私钥，并分别利用密钥控件中的交互密钥生成算法生成各自的交互密钥，再使用校验码、时间戳以及认证信息组成交互密钥信息包。

[0071] 另外，该方法在步骤 4 生成各自的传输密钥后还包括：信息发送装置 2 和信息接收装置 3 各自利用生成的传输密钥对需要传输的信息进行加解密。

[0072] 下面结合图 4 和图 5 对本发明提供的生成传输密钥的方法做进一步的详细说明。

[0073] 图 4 是依照本发明第一个实施例生成传输密钥的方法流程图，本实施例以一个简单的交互作为例子，双方指的是信息发送装置 2 和信息接收装置 3，其具体步骤如下：

[0074] 步骤 401：提出操作请求；

[0075] 步骤 402：密钥控件派发装置 1 调用控件信息生成单元 11，生成包括安全控制 ID、版本号和控件使用期限的控件信息，并调用密钥控件生成单元 12，选取两种密钥生成控件算法，例如 F(X) = 64X 和 G(X,Y) = X*Y，分别生成交互密钥生成控件和传输密钥生成控件，再将控件信息加至已生成上述两种密钥生成控件，然后加上密钥控件派发装置 1 的私钥进行签名，最终形成密钥生成控件信息包，派发至信息发送装置 2 和信息接收装置 3；所述的控件信息包括安全控制 ID，例如“NCAA.Ltd.co. 安全部”、版本号，例如“2.0.3”、控件使用

期限，例如“2009-12-01to2010-02-01”；

[0076] 步骤 403：双方主控单元 209 调用各自的签名信息认证单元 204，分别根据密钥控件派发装置 1 派发的密钥控件信息包根据已知的密钥控件派发装置 1 的公钥在本地进行解密，获取控件认证信息，所述已获取控件认证信息包括安全控制 ID“NCAA.Ltd.co. 安全部”、版本号“2.0.3”、控件使用期限“2009-12-01to2010-02-01”；

[0077] 步骤 404：双方主控单元 209 对所述控件认证信息进行合法性校验，通过验证安全控制 ID 确认接收到的信息是否为已约定的第三方 ID 内容、通过验证控件使用期限确认各自装置本地的系统时间是否在接收到的控件使用期限之内；若验证通过，则进入步骤 406，若验证未通过，交易中断，进入步骤 405；

[0078] 步骤 405：交易中断，校验未通过一方的主控单元 209 调用信息发送单元 208 向密钥控件派发装置发出重新发送的通知，结束；

[0079] 步骤 406：验证通过，信息发送装置 2 的主控单元 209 调用信息发送单元 208 向信息接收装置 3 发起密钥交互请求；步骤 406 在验证通过后还包括：双方主控单元 209 调用数据保存清理单元 204，用于保存接收到的控件信息包中的密钥控件算法信息，以保证信息的安全性；

[0080] 步骤 407：信息接收装置 3 确认接收到的请求，并与信息发送装置 2 建立 SSL 连接；

[0081] 步骤 408：双方 SSL 连接建立后，对控件版本信息进行交互：

[0082] 步骤 409：双方验证交互的版本信息是否一致，若一致，则验证通过，进行下一步；若不一致，则交易中断，双方通知各自主控单元 209 联系密钥控件派发装置 1 进行重发，结束；

[0083] 步骤 410：一致性验证通过后，双方主控单元 209 分别调用各自私钥生成单元 201 生成本地私钥，此实例中取私钥数值分别为 a = 923 和 b = 672，主控单元 209 再分别调用数据保存清理单元 207 以保证随机密钥 a 和 b 保存到本单元的安全区域内从而保证私钥的安全性；

[0084] 步骤 411：双方主控单元 209 分别调用数据保存清理单元 204 中的交互密钥算法控件，使用控件中的算法 F(X) = 64*X，根据已经生成的本地私钥分别生成各自的交互密钥数 K_a = 64*a = 59072 和 K_b = 64*b = 43008，再调用交互密钥生成单元 202，将时间戳添加至交互密钥 K_a 和 K_b，然后调用校验码认证单元 205，使用其中的“奇偶校验算法”生成校验码，以一方为例：将 K_a = 59072 和时间戳 200912122048 各位相加求和，5+9+0+7+2+2+0+0+9+1+2+1+2+2+0+4+8 = 54，是偶数所以其奇偶校验码为 0，同理可以计算出另一方奇偶校验码为 1，最后再补充控件版本信息组成各自的密钥交互密钥信息包 A = 59027|200912122048|0|2.0.3 和 B = 43008|200912122048|1|2.0.3，最后对各自的信息包进行签名；

[0085] 步骤 412：双方主控单元 209 调用各自信息发送单元 208，并通过已建立的 SSL 通信连接对密钥交互密钥信息包明文数据进行交换；

[0086] 步骤 413：双方主控单元 209 调用数据保存清理单元将接收到的对方交互密钥信息包明文数据进行存储以保证信息的安全性，再在本地对密钥交互信息进行解密从而获取交互密钥信息包中密文数据；

[0087] 步骤 414 :双方主控单元 209 分别调用各自校验码认证单元 205 和时间戳校验单元 206 对保存在数据保存清理单元 207 的密文数据进行奇偶校验和时间戳校验,校验通过则进行下一步交易,若校验未通过,则调用信息发送单元 208 联系密钥控件派发装置 1 进行重发,结束 ;

[0088] 进一步的,所述步骤 414 中的奇偶校验具体步骤为双方主控单元 209 调用校验码认证单元 205 按照步骤 411 所述奇偶校验方法对接收到的数据进行奇偶校验,通过后主控单元 209 再调用时间戳校验单元 206 对密钥交互密钥信息包的时间戳 200912122048 与当前系统时间进行比较,若时间戳所示时间大于当前系统时间 1 分钟以上则判断为超时,拒绝进一步交易 ;

[0089] 步骤 415 :双方主控单元 209 调用数据保存清理单元 207,从中取出各自的私钥 a = 923 和 b = 672,以及对方传输过来的交互密钥,调用传输密钥生成控件 203,例如 G(X,Y) = X*Y 算出最终的传输密钥 K,此实施例中 $K = a*K_b = 923*43008 = 39696384$ 和 $K = b*K_a = 672*59072 = 39696384$;

[0090] 步骤 416 :双方主控单元 209 分别调用数据发送单元 208,用所述步骤 415 中生成的传输密钥将需要传输的数据进行加密后发送给信息接受装置 3 ;

[0091] 步骤 417 :结束。

[0092] 图 5 是依照本发明第二个实施例生成传输密钥的方法流程图。本实施例以另一种算法 Diffie-Hellman (简称 DH 算法——一种公开的非对称加密算法,属于公钥密码体制) 进一步说明本发明生成传输密钥的方法。同上述第一个实施例,双方指的是信息发送装置 2 和信息接收装置 3,其具体包括以下步骤 :

[0093] 步骤 501 :提出操作请求 ;

[0094] 步骤 502 :密钥控件派发装置 1 调用控件信息生成单元 11,生成包括安全控制 ID、版本号和控件使用期限的控件信息,并调用密钥控件生成单元 12,选取两种密钥生成控件算法,例如 $F(X) = g^x \bmod n$(1 < g < n,且 g 和 n 需为较大的质数) 和 $G(X, Y) = Y^x \bmod n$,分别生成交互密钥生成控件和传输密钥生成控件,再将控件信息加至已生成上述两种密钥生成控件,然后加上密钥控件派发装置 1 的私钥进行签名,最终形成密钥生成控件信息包,派发至信息发送装置 2 和信息接收装置 3 ;所述的控件信息包括安全控制 ID,例如“FIFA.ACCA.COM.hk.”,、版本号,例如“V+2.7.0”、控件使用期限,例如“2010-01-28to2010-02-10”。

[0095] 步骤 503 :双方主控单元 209 调用各自的签名信息认证单元 204,分别根据密钥控件派发装置 1 派发的密钥控件信息包根据已知的密钥控件派发装置 1 的公钥在本地进行解密,获取控件认证信息,所述已获取控件认证信息包括安全控制 ID“FIFA.ACCA.COM.hk”、版本号“V+2.7.0”、控件使用期限“2010-01-28to2010-02-10”;

[0096] 步骤 504 :双方主控单元 209 对所述控件认证信息进行合法性校验,通过验证安全控制 ID 确认接收到的信息是否为已约定的第三方 ID 内容、通过验证控件使用期限确认各自装置本地的系统时间是否在接收到的控件使用期限之内 ;若验证通过,则进入步骤 506,若验证未通过,交易中断,进入步骤 505 ;

[0097] 步骤 505 :交易中断,校验未通过一方的主控单元 209 调用信息发送单元 208 向密钥控件派发装置发出重新发送的通知,结束 ;

[0098] 步骤 506 :验证通过,信息发送装置 2 的主控单元 209 调用信息发送单元 208 向信息接收装置 3 发起密钥交互请求 ;步骤 506 在验证通过后还包括 :双方主控单元 209 调用数据保存清理单元 204,用于保存接收到的控件信息包中的密钥控件算法信息,以保证信息的安全性 ;

[0099] 步骤 507 :信息接收装置 3 确认接收到的请求,并与信息发送装置 2 建立 SSL 连接 ;

[0100] 步骤 508 :双方 SSL 连接建立后,对控件版本信息进行交互 ;

[0101] 步骤 509 :双方验证交互的版本信息是否一致,若一致,则验证通过,进行下一步 ;若不一致,则交易中断,双方通知各自主控单元 209 联系密钥控件派发装置 1 进行重发,结束 ;

[0102] 步骤 510 :一致性验证通过后,双方主控单元 209 分别调用各自私钥生成单元 201 生成本地私钥,此实例中取私钥数值分别为 a = e 和 b = f,主控单元 209 再分别调用数据保存清理单元 207 以保证随机密钥 a 和 b 保存到本单元的安全区域内从而保证私钥的安全性 ;

[0103] 步骤 511 :双方主控单元 209 分别调用数据保存清理单元 204 中的交互密钥算法控件,使用控件中的算法 $F(X) = g^x \bmod n$(1 < g < n,且 g 和 n 需为较大的质数),根据已经生成的本地私钥分别生成各自的交互密钥数 $K^a = g^e \bmod n$ 和 $K^b = g^f \bmod n$,再调用交互密钥生成单元 202,将时间戳添加至交互密钥 K_a 和 K_b,然后调用校验码认证单元 205,使用其中的任意一种校验码生成算法生成校验码,最后再补充控件版本信息组成各自的密钥交互密钥信息包 $A = g^e \bmod n|201001051357|1$ 和 $B = g^f \bmod n|201001051357|0$,最后对各自的信息包进行签名 ;

[0104] 步骤 512 :双方主控单元 209 调用各自信息发送单元 208,并通过已建立的 SSL 通信连接对密钥交互密钥信息包明文数据进行交换 ;

[0105] 步骤 513 :双方主控单元 209 调用数据保存清理单元将接收到的对方交互密钥信息包明文数据进行存储以保证信息的安全性,再在本地对密钥交互信息进行解密从而获取交互密钥信息包中密文数据 ;

[0106] 步骤 514 :双方主控单元 209 分别调用各自校验码认证单元 205 和时间戳校验单元 206 对保存在数据保存清理单元 207 的密文数据进行奇偶校验和时间戳校验,校验通过则进行下一步交易,若校验未通过,则调用信息发送单元 208 联系密钥控件派发装置 1 进行重发,结束 ;

[0107] 进一步的,所述步骤 514 所述奇偶校验具体步骤为双方主控单元 209 调用校验码认证单元 205 按照步骤 511 所述奇偶校验方法对接收到的数据进行奇偶校验,通过后主控单元 209 再调用时间戳校验单元 206 对密钥交互密钥信息包的时间戳 201001051357 与当前系统时间进行比较,若时间戳所示时间大于当前系统时间 1 分钟以上则判断为超时,拒绝进一步交易 ;

[0108] 步骤 515 :双方主控单元 209 调用数据保存清理单元 207,从中取出各自的私钥 a = e 和 b = f,以及对方传输过来的交互密钥,调用传输密钥生成控件 203,例如 $G(X,Y) = Y^x \bmod n$,算出最终的传输密钥 K,此实施例中 $K = [K_b]^a \bmod n = [g^f \bmod n]^e \bmod n = (g^f)^e \bmod n, = g^{f*e} \bmod n$ 和 $K = [K_a]^b \bmod n = [g^e \bmod n]^f \bmod n = (g^e)^f \bmod n, = g^{e*f} \bmod n$;

[0109] 步骤 516 :双方主控单元 209 分别调用数据发送单元 208,用所述步骤 417 中生成的传输密钥将需要传输的数据进行加密后发送给信息接受装置 3 ;

[0110] 步骤 517 :结束。

[0111] 以上所述的具体实施例,对本发明的目的、技术方案和有益效果进行了进一步详细说明,所应理解的是,以上所述仅为本发明的具体实施例而已,并不用于限制本发明,凡在本发明的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

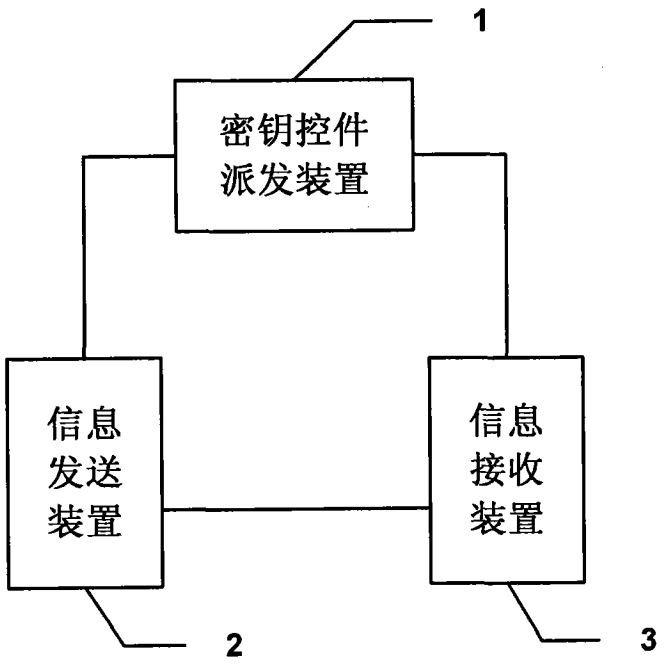

1
密钥控件派发装置
信息发送装置
信息接收装置
2
3

图 1

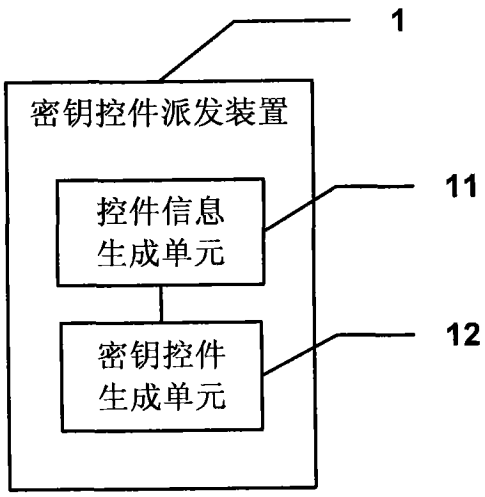

1
密钥控件派发装置
控件信息生成单元
11
密钥控件生成单元
12

图 2

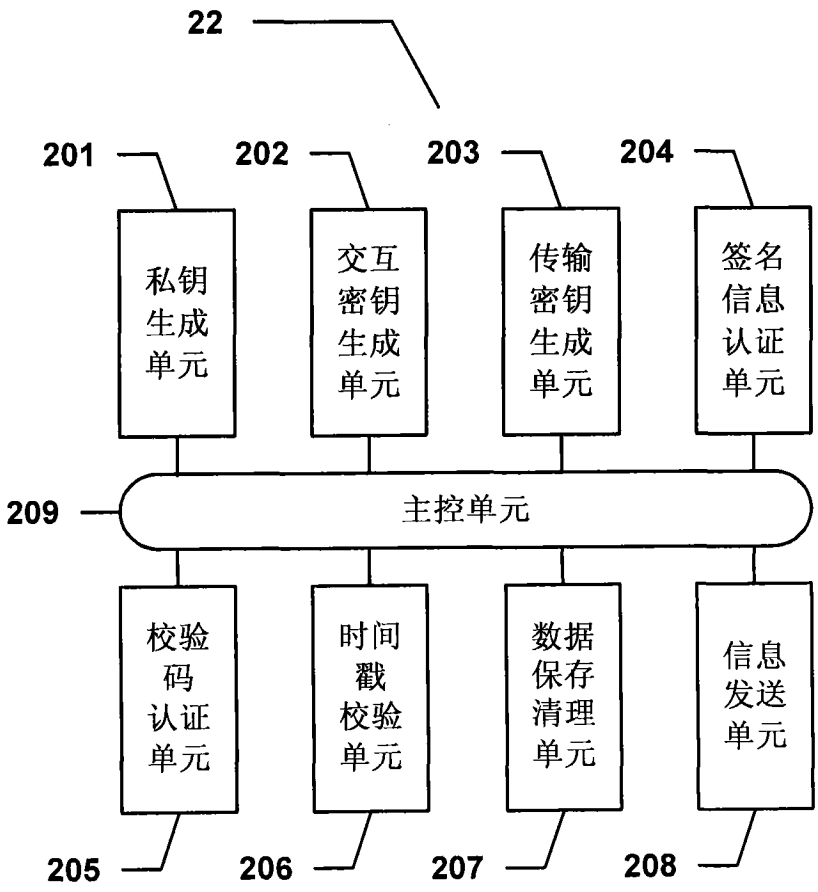

22
201
202
203
204
私钥生成单元
交互密钥生成单元
传输密钥生成单元
签名信息认证单元
209
主控单元
校验码认证单元
时间戳校验单元
数据保存清理单元
信息发送单元
205
206
207
208

图 3

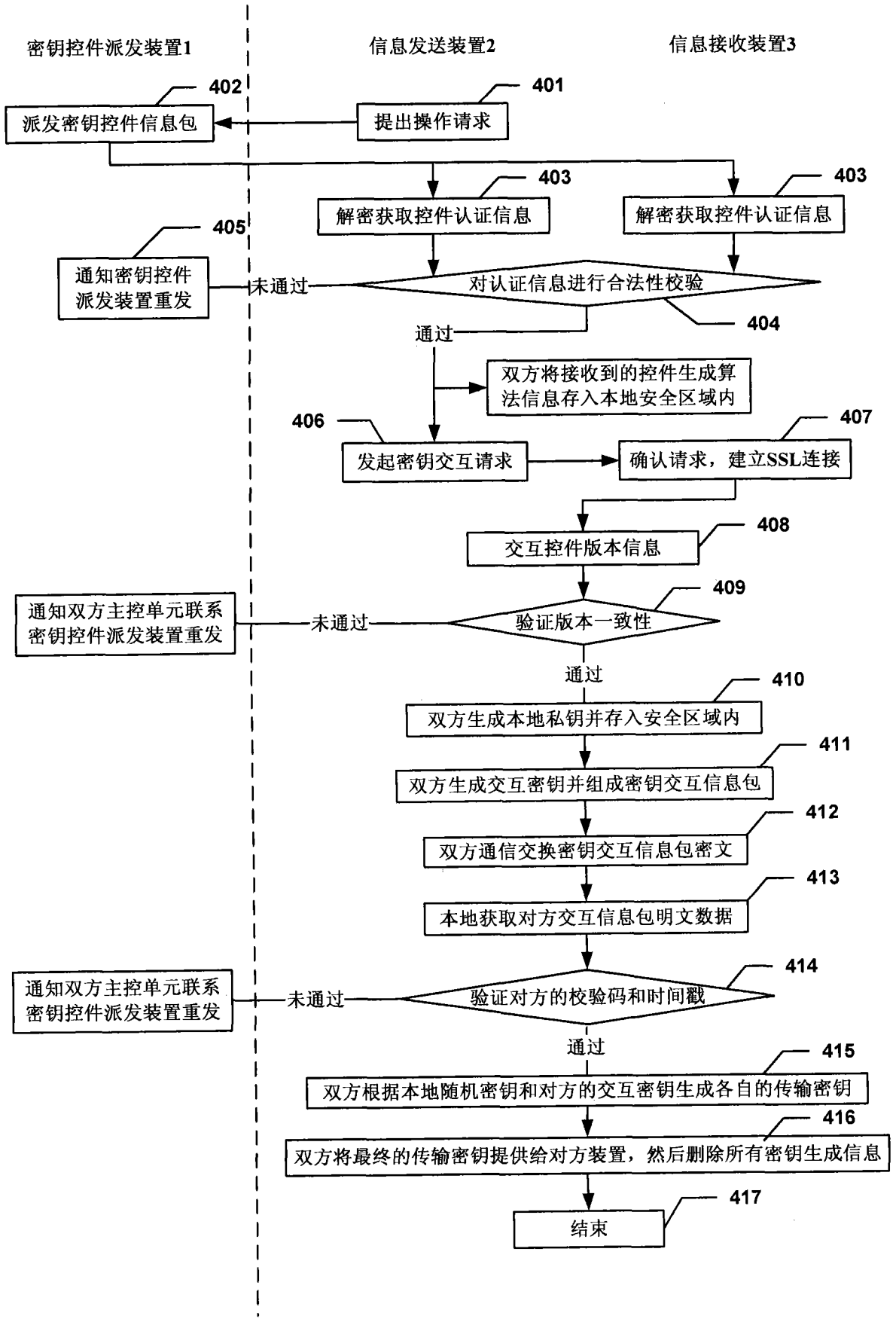

密钥控件派发装置1
信息发送装置2
信息接收装置3
402
派发密钥控件信息包
401
提出操作请求
403
解密获取控件认证信息
403
解密获取控件认证信息
405
通知密钥控件派发装置重发
未通过
对认证信息进行合法性校验
404
通过
双方将接收到的控件生成算法信息存入本地安全区域内
406
发起密钥交互请求
407
确认请求，建立SSL连接
408
交互控件版本信息
通知双方主控单元联系密钥控件派发装置重发
未通过
409
验证版本一致性
通过
410
双方生成本地私钥并存入安全区域内
411
双方生成交互密钥并组成密钥交互信息包
412
双方通信交换密钥交互信息包密文
413
本地获取对方交互信息包明文数据
通知双方主控单元联系密钥控件派发装置重发
未通过
414
验证对方的校验码和时间戳
通过
415
双方根据本地随机密钥和对方的交互密钥生成各自的传输密钥
416
双方将最终的传输密钥提供给对方装置，然后删除所有密钥生成信息
417
结束

图 4

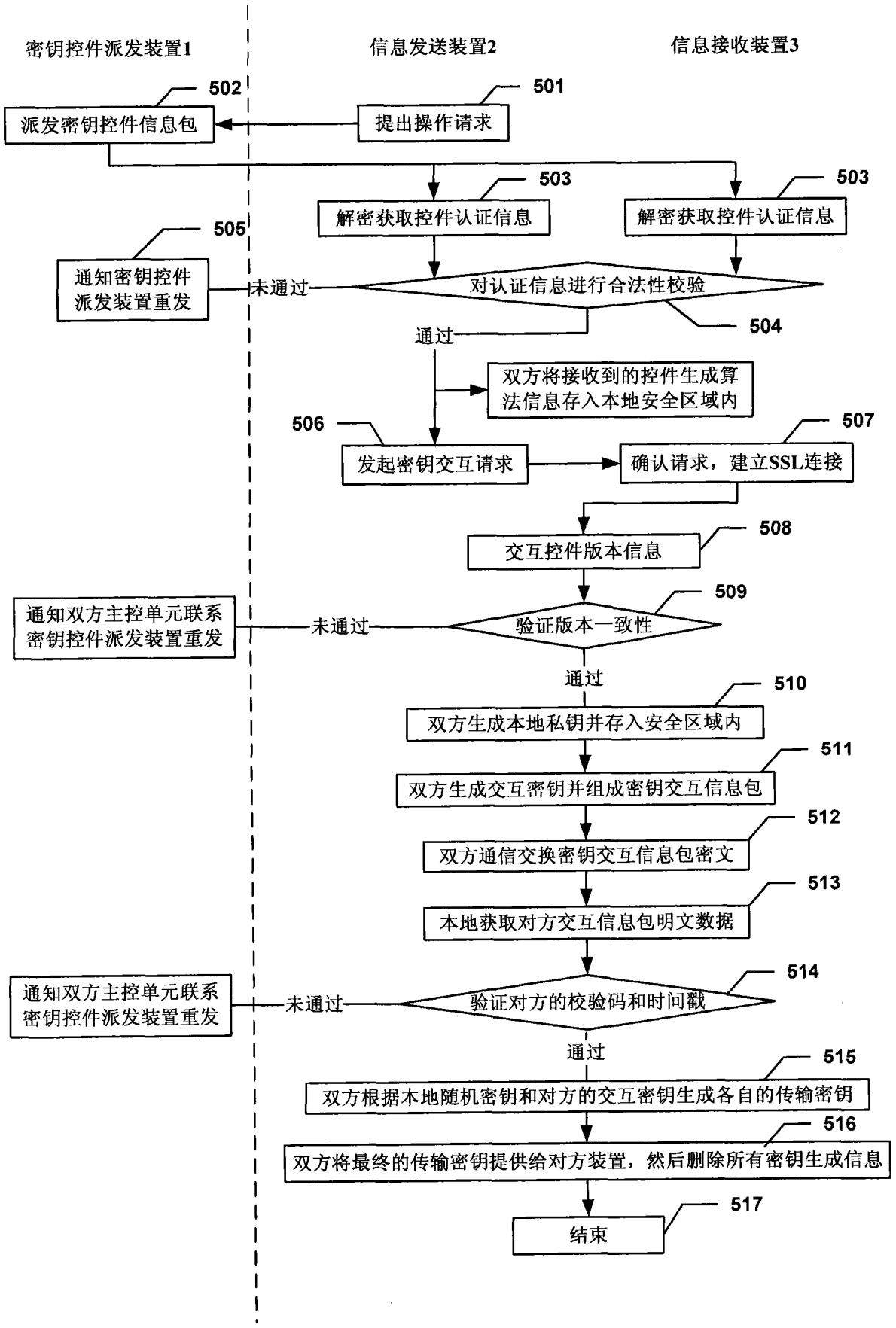

密钥控件派发装置1
信息发送装置2
信息接收装置3
502
派发密钥控件信息包
501
提出操作请求
503
解密获取控件认证信息
503
解密获取控件认证信息
505
通知密钥控件派发装置重发
未通过
对认证信息进行合法性校验
504
通过
双方将接收到的控件生成算法信息存入本地安全区域内
506
发起密钥交互请求
507
确认请求，建立SSL连接
508
交互控件版本信息
509
通知双方主控单元联系密钥控件派发装置重发
未通过
验证版本一致性
通过
510
双方生成本地私钥并存入安全区域内
511
双方生成交互密钥并组成密钥交互信息包
512
双方通信交换密钥交互信息包密文
513
本地获取对方交互信息包明文数据
514
通知双方主控单元联系密钥控件派发装置重发
未通过
验证对方的校验码和时间戳
通过
515
双方根据本地随机密钥和对方的交互密钥生成各自的传输密钥
516
双方将最终的传输密钥提供给对方装置，然后删除所有密钥生成信息
517
结束

图 5

	安全控制 ID	版本号	控件使用期限
实施例 1	NCAA.Ltd.co.安全部	2.0.3	2009-12-01to2010-02-01
实施例 2	FIFA.ACCA.COM.hk.	V+ 2.7.0	2010-01-28to2010-02-10

图 6