(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 103428692 B
(45)授权公告日 2016.08.10

(21)申请号 201310343147.6

(22)申请日 2013.08.07

(73)专利权人 华南理工大学
地址 510641 广东省广州市天河区五山路381号

(72)发明人 何道敬 唐韶华 贺品嘉

(74)专利代理机构 广州市华学知识产权代理有限公司 44245
代理人 蔡茂略

(51)Int.Cl.
H04W 12/04(2009.01)
H04W 12/06(2009.01)
H04W 12/08(2009.01)

(56)对比文件
EP 1833222 A1,2007.09.12,
CN 101335625 A,2008.12.31,
H. Guo等.A unique batch authentication protocol for vehicle-to-grid communications.《IEEE Transactions on Smart Grid》.2011, 第2卷(第4期),
何道敬. 无线网络安全的关键技术研究.《浙江大学2012年博士毕业论文》.2012,

审查员 徐意特

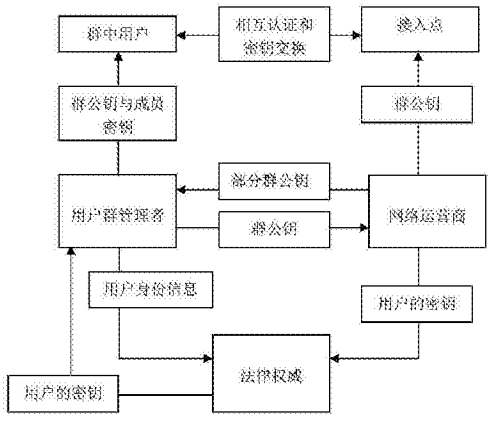
权利要求书2页 说明书11页 附图2页

(54)发明名称

可问责且隐私保护的无线接入网络认证方法及其认证系统

(57)摘要

本发明公开了一种可问责且隐私保护的无线接入网络认证方法,包括以下步骤:步骤1、用户群管理者在网络运营商处注册;步骤2、用户和用户群管理者联系以进行认证,使用户成为群中用户;步骤3、若发现用户被攻破,网络运营商撤销被攻破用户;步骤4、用户成功接入无线网络;步骤5、当接入点处有两个或两个以上签名需要认证时,接入点对这些签名进行批量签名验证;步骤6、法律权威确定对特定通信会话负责的用户。本发明还公开了一种实现可问责且隐私保护的无线接入网络认证方法的认证系统,包括:网络运营商、接入点、用户群管理者、群中用户和法律权威。具有使每一个实体项的信任度都有限,有效避免了代管问题与单点失效问题。



CN 103428692 B

1.一种可问责且隐私保护的无线接入网络认证方法，其特征在于，包括以下步骤：

步骤1、用户群管理者在网络运营商处注册，网络运营商生成群私钥以及部分群公钥，并将部分群公钥发给用户群管理者；用户群管理者根据部分群公钥生成群公钥后并把群公钥发给网络运营商，网络运营商把从用户群管理者处收到的群公钥广播至接入点；

步骤2、用户和用户群管理者联系以进行认证，用户群管理者将向其发送用于接入网络的成员密钥和群公钥，此时用户成功加入用户群，成为群中用户；

步骤3、若发现用户被攻破，则用户群管理者将把这些被攻破用户视为需撤销的用户，并把撤销用户的名单列表发送给网络运营商，网络运营商将所述名单广播给接入点，以撤销所述被攻破用户；

步骤4、接入点的通信范围内的用户与所述接入点进行相互认证和密钥交换后，建立共享的对称密钥，所述对称密钥用于通信会话，此时用户成功接入无线网络；

步骤5、当接入点处有两个或两个以上签名需要认证时，接入点对这些签名进行批量签名验证；

步骤6、若法律权威需要追踪对特定通信会话负责的用户，只需从网络运营商处获取群私钥，并从用户群管理者处获取对特定通信会话负责的用户的成员密钥和用户身份信息的映射对，利用所述获取的群私钥与映射对来确定对特定通信会话负责的用户；

所述步骤4包括以下步骤：

①接入点周期性地广播具有本接入点数字签名的信标消息，以表示所述接入点处于服务状态；

②用户收到所述信标消息后，根据所述信标消息验证时间戳的有效性、接入点的证书过期时间以及接入点的公钥的真实性；若时间戳的有效性、接入点的证书过期时间或公钥的真实性任一项未通过验证，则用户拒绝链接接收到信标信息所对应的接入点；若时间戳的有效性、接入点的证书过期时间以及接入点的公钥的真实性全部通过验证，则用户生成请求信息，并利用自己的成员密钥对其进行群签名，并单播回复给接入点；

③接入点收到用户发来的步骤②所述的请求信息后，先检查信息的新鲜性，再检查该用户是否存在于撤销用户的名单列表内；若存在，则拒绝链接；否则，计算得到与用户共享的对称密钥并发送应答信息给用户；

④用户在接收到步骤③中所述的接入点发来的信息后，验证该信息是否有效，若信息无效，则拒绝链接；否则，建立链接。

2.根据权利要求1所述的可问责且隐私保护的无线接入网络认证方法，其特征在于，所述步骤6包括以下步骤：

A、法律权威要求网络运营商与用户群管理者追踪对特定通信会话负责的用户；

B、网络运营商基于网络链接及会话标识，从网络日志文件中找到相应的会话认证信息；

C、网络运营商对步骤B所述的会话认证信息中的数字签名的前三个元素进行线性加密，并用群私钥来获得该用户的成员密钥；此后，网路运营商把获取的该用户的成员密钥报告给法律权威；

D、法律权威向用户群管理者发送从网络运营商处获得的成员密钥；

E、用户群管理者根据从法律权威处获得的成员密钥，在自己存储的成员密钥和用户身

份信息的映射对中查找，并把查到的用户身份信息回复给法律权威。

3.一种实现权利要求1所述可问责且隐私保护的无线接入网络认证方法的认证系统，其特征在于，包括：网络运营商、接入点、用户群管理者、群中用户和法律权威；所述网络运营商向用户群管理者发送部分群公钥并从用户群管理者处接收群公钥，网络运营商还向接入点广播群公钥；接入点与群中用户进行相互认证与密钥交换，群中用户还从用户群管理者处获取用于接入网络的成员密钥与群公钥；法律权威从网络运营商处获得群私钥，并从用户群管理者处获取成员密钥和用户身份信息的映射对。

可问责且隐私保护的无线接入网络认证方法及其认证系统

技术领域

[0001] 本发明涉及一种无线通信技术，特别涉及一种可问责且隐私保护的无线接入网络认证方法及其认证系统。

背景技术

[0002] 无线接入网络的普及极大地改善了生活的质量与工作的效率，让用户几乎可以随时随地接入网络。而随着对无线接入网络的需求越来越大，无线接入网络开始在生活中扮演起不可替代的角色。但令人担忧的是，无线接入网络中风险无处不在，这些风险包括缺乏经验或无警觉性的用户的敏感信息泄露、无线信号拦截的易实现性和快速趋于成熟的监控设备等。所以，若需要大范围部署这种无线接入网络，安全性、隐私性、可问责性与高效性是需要考虑的最主要的问题。然而，在现有技术中，实际可用的可问责且隐私保护的无线接入网络认证系统却少之又少。另外，现有的大多数确保隐私性的认证系统都需要一个可信任的第三方。然而，在可信任的第三方存在时，系统会面临代管问题与单点失效问题。敌手可通过破坏可信任的第三方来破坏整个系统的配置。因此，在不涉及可信任的第三方的前提下，同时保证无线接入网络认证系统的可问责性、安全性、隐私性与高效性就显得十分必要。除此之外，问责性和隐私性是两个看似矛盾的目标，因此现有技术无法被直接应用到无线接入网络认证系统中，从而向系统提供可问责性的同时不失去系统的隐私性。而本发明基于职责分离原则，很好地解决了这个问题。在本发明中，网络运营商拥有群私钥(group private key，下同)，但不知道成员密钥(member secret keys，下同)和用户身份信息的映射对，而用户群管理者(group manager，下同)知道成员密钥和用户身份信息的映射对(the mapping between the member secret keys and the essential attributes of the users，下同)，但却没有群私钥，这保证了系统的隐私性。而在法律权威的需要下，网络运营商和用户群管理者可共同提供信息，以找出需负责的用户，这保证了可问责性。本发明在不涉及到一个可信任的第三方的前提下，同时保证了系统的安全性、隐私性、可问责性和高效性，这是现有技术无法实现的。

[0003] 现有的无线接入认证系统涉及三方：一个无线漫游用户U，一个访问接入点AP和网络运营商NO。一定数量的AP部署在服务区域的不同地点，以覆盖整个区域，并向网络用户提供网络服务。用户可用他们的移动设备在任意地点接入该网络。现有的无线接入网络认证方法及其认证系统主要有两个缺点。首先，现有方法及其系统往往需要一个可信任的第三方，如成员管理者、信任权威(Trust Authority，下同)、本地服务器、脱机安全管理者和AAA服务器。这个可信任的第三方管理所有的密钥资料。但若这些密钥资料泄露出去的话，用户的隐私会面临被公开的危险。不幸的是，在有可信任的第三方时，安全系统会面临代管问题和单点失效问题。敌手可通过破坏可信任的第三方来破坏整个系统的配置。第二，现有无线接入网络无法在提供可问责性的同时保证隐私性。若想让法律权威可找到对特定通信会话负责的用户，则用户信息会或多或少被泄露；但若想保证用户的隐私性，则法律权威难以根据有限的信息对用户进行追踪。更重要的是，提供可问责性的同时不失去隐私性，这是两个

看似矛盾的目标。现在没有可以直接部署并可达成以上目标的可用的隐私相关(privacy aware)密码原语。

发明内容

[0004] 本发明的首要目的在于克服现有技术的缺点与不足，提供一种可问责且隐私保护的无线接入网络认证方法，该方法有效地避免了代管问题和单点失效的问题。

[0005] 本发明的另一目的在于克服现有技术的缺点与不足，提供一种实现可问责且隐私保护的无线接入网络认证方法的认证系统，该系统不涉及可信任的第三方，安全性高，隐私性高。

[0006] 本发明的首要目的通过下述技术方案实现：一种可问责且隐私保护的无线接入网络认证方法，包括以下步骤：

[0007] 步骤1、用户群管理者在网络运营商处注册，网络运营商生成群私钥以及部分群公钥(partial group public key，下同)，并将部分群公钥发给用户群管理者；用户群管理者生成群公钥(group public key，下同)后发还给网络运营商；网络运营商把从用户群管理者处收到的群公钥广播至每一个接入点；

[0008] 步骤2、用户本人和用户群管理者联系以进行认证，此后用户群管理者将向其发送用于接入网络的一个成员密钥和群公钥；此时用户成功加入用户群，成为群中用户；

[0009] 步骤3、若发现用户被攻破，则用户群管理者将把这些被攻破用户视为需撤销的用户，并把撤销用户的列表发送给网络运营商；网络运营商在此名单上数字签名后广播给每一个接入点，以撤销被攻破用户；此时，用户被撤销；

[0010] 步骤4、用户若要接入网络，首先需要保证自己处于一个接入点的通信范围内；在与该接入点进行相互认证与密钥交换后，接入点与用户间会建立起一个共享对称密钥，用于往后的通信会话；此时，用户成功接入无线网络；

[0011] 步骤5、当接入点处有两个或两个以上签名需要认证时，接入点对这些签名进行批量签名验证。我们的批量签名验证技术在极大地减少了验证大量签名所消耗的时间的同时，还减少了接入点处签名验证这一潜在的瓶颈问题所导致的连接中断率。

[0012] 步骤6、若法律权威想追踪对特定通信会话负责的用户，只需从网络运营商处获得群私钥，并从用户群管理者处获取成员密钥和用户身份信息的映射对；利用群私钥与上述映射对可确定用户。

[0013] 所述步骤4包括以下步骤：

[0014] A、接入点周期性地广播有该接入点数字签名的信标消息，从而宣布其服务存在；

[0015] B、当用户收到信标消息后，会根据信标消息，验证时间戳的有效性、接入点的证书过期时间以及其公钥的可靠性。若这些验证有任意一个未通过，用户将不会链接该接入点；若这些验证全部通过，用户生成请求信息，并利用自己的成员密钥对其进行群签名，并单播回复给接入点；

[0016] C、当接入点收到用户发来的上述信息后，将先检查信息的新鲜性(message freshness，下同)。随后，检查该用户是否存在其撤销用户的列表内。若存在，则拒绝链接；若不存在，则计算得到与其共享的对称密钥并发送应答信息给用户；

[0017] D、用户在接收到上述接入点发来的信息后，会验证该信息的有效性。若信息无效，

则拒绝链接;若有效,则该链接成功建立。

[0018] 所述步骤6包括以下步骤:

[0019] (1)法律权威要求追踪对特定通信会话负责的用户;

[0020] (2)网络运营商基于网络链接及会话标识,从网络日志文件中找到相应的会话认证信息;

[0021] (3)网络运营商对上述会话认证信息中的数字签名的前三个元素进行线性加密,并用群私钥来获得该用户的成员密钥。此后,网路运营商把获取的该用户的成员密钥报告给法律权威;

[0022] (4)法律权威向用户群管理者发送从网络运营商处获得的该用户的成员密钥;

[0023] (5)用户群管理者根据从法律权威处获得的该用户的成员密钥,在自己存储的成员密钥和用户身份信息的映射对中查找,并把查到的用户身份信息回复给法律权威。

[0024] 本发明的网络认证方法具有以下六个阶段:系统建立、添加新用户、撤销用户、相互认证与密钥交换、批量签名验证、用户追踪。在系统建立阶段,网络运营商和每个用户群管理者各自生成部分群公钥。群公钥被分配给每一个接入点。系统在有新用户入群时进入添加新用户阶段,而当一个或多个用户被撤销时进入撤销用户阶段。在相互认证与密钥交换阶段,如一个用户想链接到一个接入点,他/她需要与接入点间进行相互认证与密钥交换,然后建立一个共享对称密钥。在批量签名验证阶段,接入点可同时验证许多接收到的请求,而不是单独地处理每一个请求。在用户追踪阶段,网络运营商和用户群管理者帮助法律权威追踪一个对特定网络链接负责的用户。

[0025] 本发明的另一目的通过以下技术方案实现:一种实现可问责且隐私保护的无线接入网络认证方法的认证系统,其特征在于,包括:网络运营商、接入点、用户群管理者、群中用户和法律权威;所述网络运营商向用户群管理者发送部分群公钥并从用户群管理者处接收群公钥,网络运营商还向接入点广播群公钥;接入点与群中用户进行相互认证与密钥交换,群中用户还从用户群管理者处获取用于接入网络的成员密钥与群公钥;法律权威从网络运营商处获得群私钥,并从用户群管理者处获取成员密钥和用户身份信息的映射对。

[0026] 本发明的认证系统中的密钥管理模型共涉及四个典型的网络实体:网络运营商、接入点、用户群管理者和群中用户。在本发明中,用户并不直接向网络运营商进行注册,而是由用户群管理者代表所有其群内用户向网络运营商订阅服务。网络运营商生成群私钥和部分的群公钥,但对群私钥进行保密。当收到一个群管理者的注册请求时,网络运营商会把部分群公钥分发给这个用户群管理者。然后,群管理者生成群公钥并将其返回给网络运营商。最后,网络运营商把群公钥发送给每个接入点。若要接入网络,每个用户需要向其群管理者请求其成员密钥和群公钥。

[0027] 这种密钥管理方案有几个突出的特征,首先,对于控制接入的目的来说,每一个合法的拥有有效成员密钥的用户可生成一个有效的接入证书,例如新接入请求的群签名。每个接入点都可用群公钥对该接入证书进行验证。因此,接入安全得到保证。第二,本发明把群私钥和成员密钥和用户身份信息的映射对分别保存在两个自主的实体项中:群用户管理者和网络运营商。其中网络运营商拥有群私钥,但不知道映射对。而群管理者知道映射对,却不知道群私钥。在这里,假设群管理者不会与网络运营商串通。这个假设是合理的,因为用户群管理者和网络运营商基本来自不同的群,而且他们之间甚至有利益冲突。这导致了

用户群管理者与网络运营商都不能确定特定用户的身份信息也不能利用用户的接入认证来侵犯用户的隐私。因此，用户的隐私性得到了加强。

[0028] 最后，在网络运营商和用户群管理者的共同帮助下，有且仅有法律权威可以根据任意的通信链接追踪到相应的网络用户。因此，在发生服务纠纷或欺诈时，法律权威可以精准地确定需负责任的用户，并追求其责任。所以，用户问责也能够实现。同时，整个密钥管理过程都可以在系统建立时完成，因此这不会在其后带来任何计算与通信的开销。

[0029] 通过修改密钥生成算法开发了新的短群签名(Short group signature，下同)方案。其后，将新型群签名集成到本发明的认证和密钥管理协议的设计中。除此以外，为了实现高效性，基于新型群签名，提出了新型的批量签名验证方法。为了撤销一个被攻破的用户，采用了Verifier-Local Revocation(本地验证吊销)方法。这个方法是基于新型群签名方案设计的。除此之外，为了支持系统的更新和大规模的用户撤销，一些附加的机制也被合并至了本发明中。

[0030] 本发明的可问责且隐私保护的高效无线接入网络系统，包括：在系统建立阶段，用户群管理者在网络运营商处注册，网络运营商生成群私钥以及部分群公钥，并将部分群公钥发给用户群管理者；用户群管理者生成群公钥后发还给网络运营商，随后网络运营商将群公钥广播至每一个接入点。在添加新用户阶段，用户本人和用户群管理者联系以进行认证，此后用户将获得用于接入网络的一个成员密钥和群公钥。若发现用户被攻破，用户群管理者将把这些被攻破用户视为需撤销的用户，并把撤销用户的列表发送给网络运营商，网络运营商在此名单上数字签名后广播给每一个接入点，以撤销被攻破用户。用户若要接入网络，首先需要保证自己处于一个接入点的通信范围内；在与该接入点进行相互认证与密钥交换后，接入点与用户间会建立起一个共享对称密钥，用于往后的通信会话。若法律权威想追踪对特定通信会话负责的用户，只需从网络运营商处获得群私钥，并从用户群管理者处获取成员密钥和用户身份信息的映射对；利用群私钥与上述映射对可确定用户。

[0031] 本发明是首个同时支持无线接入网络可问责性、安全性、隐私性和高效性的系统。以往系统没做到的一点是，在提供可问责性的同时保证系统的隐私性。但在本发明中，网络运营商拥有群私钥，但不知道成员密钥和用户身份信息的映射对；而用户群管理者知道成员密钥和用户身份信息的映射对，却没有群私钥；这保证了隐私性。而在法律权威的要求下，网络运营商和用户群管理者可共同提供信息，以找出需负责的用户，这提供了可问责性。本发明支持系统的更新和大规模的用户撤销，这保证了系统的高效性。除此以外，本发明的另一特点是不依赖于任何可信任的第三方。在本发明中，每一个实体项的信任度都是有限的，这使系统避免了代管问题与单点失效问题。

[0032] 本发明的工作原理：本发明提出了一种可问责且隐私保护的无线接入网络认证系统。在该系统中，共有六个阶段，分别为系统建立、添加新用户、撤销用户、相互认证与密钥交换和、批量签名验证、用户追踪。首先，系统需要初始化，这便是系统建立的阶段。在这个阶段，系统完成群公钥分配的任务。系统成功建立后，每一个接入点都分有一份群公钥。此后，若要添加新用户，则进入添加新用户阶段；若要撤销用户，则进入撤销用户阶段。在用户想链接到接入点时，需与该接入点进行相互认证与密钥交换，这时进入相互认证与密钥交换阶段。而当法律权威需要追踪一个特定用户时，系统进入用户追踪阶段。本发明在不涉及到一个可信任的第三方的前提下，同时保证了系统的安全性、隐私性、可问责性和高效性。

首先，对于控制接入的目的来说，每一个合法的拥有有效成员密钥的用户可生成一个有效的接入证书，例如新接入请求的群签名。每个接入点都可用群公钥对该接入证书进行验证。因此，接入安全得到保证。第二，本发明把成员密钥与用户身份信息之间的映射对以及群私钥分别保存在两个自主的实体项中：用户群管理者和网络运营商。其中网络运营商拥有群私钥，但不知道成员密钥与用户身份信息之间的映射对。而用户群管理者知道映射对，却不知道群私钥。在这里，假设群管理者不会与网络运营商串通。这个假设是合理的，因为用户群管理者和网络运营商基本来自不同的群，而且他们之间甚至有利益冲突。这导致了用户群管理者与网络运营商都不能确定特定用户的身份信息也不能利用用户的接入认证来侵犯用户的隐私。因此，系统的隐私性得到了保证。第三，在网络运营商和用户群管理者的共同帮助下，有且仅有法律权威可以根据任意的通信链接追踪到相应的网络用户。因此，在发生服务纠纷或欺诈时，法律权威可以精准地确定需负责任的用户，并追求其责任。所以，用户问责也能够实现。同时，整个密钥管理过程都可以在系统建立时完成，因此这不会在其后系统的长期运行过程带来任何计算与通信的开销。最后，通过修改密钥生成算法开发了不同的短群签名方案。其后，将新型群签名集成到本发明的认证和密钥管理协议的设计中。除此以外，基于新型群签名，提出了新型的批量签名验证方法。为了撤销一个被攻破的用户，采用了Verifier-Local Revocation(本地验证吊销)方法。这个方法是基于新型群签名方案设计的。除此之外，为了支持系统的更新和大规模的用户撤销，一些附加的机制也被合并至了本发明中。因此，系统的高效性得到保证。

[0033] 本发明相对于现有技术具有如下的优点及效果：

[0034] 1、本发明不依赖于任何可信任的第三方，每一个实体项的信任度都是有限的，这避免了代管问题和单点失效问题。

[0035] 2、本发明特别适用于无线接入网络，它基于职责分离原则与可实现的批量签名验证的新群签名算法的整合。

[0036] 3、本发明通过实现用户和接入点之间明确的相互认证与密钥建立，保证了系统的安全性。

[0037] 4、本发明通过实现用户与接入点之间单方向上的匿名认证，保证了用户的匿名性与不可链接性。

[0038] 5、本发明在提供可问责性的同时不失去隐私性。因为网络运营商拥有群私钥，但不知道映射对，而用户群管理者知道映射对，但却没有群私钥，这保证了隐私性。而在法律权威的需要下，网络运营商和用户群管理者可共同提供信息，以找出需负责的用户，这保证了可问责性。

[0039] 6、本发明通过采用Verifier-Local Revocation(本地验证吊销)方法与一些附加机制，支持系统的更新和大规模的用户撤销，保证了系统的高效性。

[0040] 7、本发明允许新用户的动态添加与被攻破用户的动态撤销。本发明是首个同时支持无线接入网络可问责性、安全性、隐私性和高效性的系统。

附图说明

[0041] 图1是本发明的流程图

[0042] 图2是本发明的信任与密钥管理模型示意图。

具体实施方式

[0043] 下面结合实施例及附图对本发明作进一步详细的描述，但本发明的实施方式不限于此。

[0044] 实施例

[0045] 现有的无线接入认证系统涉及三方：一个无线漫游用户U，一个访问接入点AP和网络运营商NO。一定数量的AP部署在服务区域的不同地点，以覆盖整个区域，并向网络用户提供网络服务。用户可用他们的移动设备在任意地点接入该网络。

[0046] 图2为本发明的无线接入网络认证系统，本发明的认证系统中的密钥管理模型共涉及四个典型的网络实体：网络运营商、接入点、用户群管理者和群中用户。在本发明中，用户并不直接向网络运营商进行注册，而是由用户群管理者代表所有其群内用户向网络运营商订阅服务。网络运营商生成群私钥和部分的群公钥，但对群私钥进行保密。当收到一个群管理者的注册请求时，网络运营商会把部分群公钥分发给这个用户群管理者。然后，群管理者生成群公钥并将其返回给网络运营商。最后，网络运营商把群公钥发送给每个接入点。若要接入网络，每个用户需要向其群管理者请求其成员密钥和群公钥。

[0047] 这种密钥管理方案有几个突出的特征。首先，对于控制接入的目的来说，每一个合法的拥有有效成员密钥的用户可生成一个有效的接入证书，例如新接入请求的群签名。每个接入点都可用群公钥对该接入证书进行验证。因此，接入安全得到保证。第二，本发明把群私钥和成员密钥和用户身份信息的映射对分别保存在两个自主的实体项中：群管理者和网络运营商。其中网络运营商拥有群私钥，但不知道映射对。而群管理者知道映射对，却不知道群私钥。在这里，假设群理者不会与网络运营商串通。这个假设是合理的，因为用户群管理者和网络运营商基本来自不同的群，而且他们之间甚至有利益冲突。这导致了用户群管理者与网络运营商都不能确定特定用户的身份信息也不能利用用户的接入认证来侵犯用户的隐私。因此，用户的隐私性得到了加强。

[0048] 最后，在网络运营商和用户群管理者的共同帮助下，有且仅有法律权威可以根据任意的通信链接追踪到相应的网络用户。因此，在发生服务纠纷或欺诈时，法律权威可以精准地确定需负责任的用户，并追求其责任。所以，用户问责也能够实现。同时，整个密钥管理过程都可以在系统建立时完成，因此这不会在其后带来任何计算与通信的开销。

[0049] 本发明通过修改密钥生成算法开发了新的短群签名(short group signature)方案。其后，将新型群签名集成到本发明的认证和密钥管理协议的设计中。除此以外，为了实现高效性，基于新型群签名，提出了新型的批量签名验证方法。为了撤销一个被攻破的用户，采用了Verifier-Local Revocation(本地验证吊销)方法。这个方法是基于新型群签名方案设计的。除此之外，为了支持系统的更新和大规模的用户撤销，一些附加的机制也被合并至了本发明中。

[0050] 本发明由以下六个阶段组成：系统建立、添加新用户、撤销用户、相互认证与密钥交换、批量签名验证以及用户追踪。在系统建立阶段，网络运营商和每个用户群管理者各自生成部分群公钥。群公钥被分配给每一个接入点。系统在有新用户入群时进入添加新用户阶段，而当一个或多个用户被撤销时进入撤销用户阶段。在相互认证与密钥交换阶段，如一个用户想链接到一个接入点，他/她需要与接入点间进行相互认证，然后建立一个共享对称

密钥。在批量签名验证阶段，接入点可同时验证许多接收到的请求，而不是单独地处理每一个请求。在用户追踪阶段，网络运营商和用户群管理者帮助法律权威追踪一个对特定网络链接负责的用户。

[0051] 如图1所示，实现本发明的无线接入网络认证系统的认证方法的六个阶段具体如下：

[0052] A.系统建立阶段

[0053] 网络运营商负责的是所有用户群的群私钥和部分群公钥的生成操作。网络运营商处理的详细过程如下：

[0054] 1.选择一个随机的生成元$g_2 \in G_2$，并计算$g_1=\psi(g_2)$。

[0055] 2.随机选取$\eta \in G_1 \setminus \{1_{G_1}\}$，$s_1, s_2 \in Z_p$且设置$u, v \in G_1$，$s_1 u = s_2 v = \eta$，可求出$u=s_1^{(-1)}\eta$，$v=s_2^{(-1)}\eta$。其中$s_1^{(-1)}$是$s_1$的倒数，$s_2^{(-1)}$是$s_2$的倒数。

[0056] 3.将群私钥$gsk=(s_1,s_2)$保密。

[0057] 4.随机选择$h_0 \in G_2 \setminus \{1_{G_2}\}$并设置$h_1, h_2 \in G_2$，$h_1=s_1 \cdot h_0$，$h_2=s_2 \cdot h_0$。

[0058] 5.网络运营商一旦收到群身份为grp_i的群管理者GM_j的注册请求信息，网络运营商需对群管理者GM_j进行认证。这个认证基于已建立好的群管理者与网络运营商之间的信任关系。这种信任关系可能是在本人接触时建立的。然后网络运营商随机选择$j \in Z_p$作为该用户群的群索引并储存配对(j, grp_j)。接下来网络运营商向群管理者发送信息$(j, g_1, g_2, \eta, u, v)$，其中$(g_1, g_2, \eta, u, v)$是部分群公钥。在本发明中，网络运营商使用一个安全传输协议(如有线传输层安全协议)与群管理者GM_j进行通信。设想strong Diffie-Hellman(SDH)在(G_1, G_2)上是保持的，而linear Diffie-Hellman在G_1上是保持的。

[0059] 为了改进所提出系统的效率，网络运营商分发给每个群的系统参数h_0和部分群公钥(g_1, g_2, η)是一样的。为了实现不可否认性，在上述第5步中，网络运营商在标准数字签名方案下对信息$(j, g_1, g_2, \eta, u, v)$签名。相关的数字签名方案有RSA和ECDSA。值得注意的是，群管理者在网络运营商处注册后，网络运营商可向群管理者发送它的公钥。因此，不需要公钥体系(PKI)。假设本发明使用了ECDSA-160。这个网络运营商的数字签名公/私钥对被定义为(OPK,OSK)。

[0060] 每个群管理者GM_j在收到$(j, g_1, g_2, \eta, u, v)$后，将按照如下步骤生成群公钥：

[0061] 1.随机选择一个数字$\gamma \in Z_p$，并设置$w_j=\gamma g_2$。

[0062] 2.返回信息(j, gpk_j)给网络运营商，其群公钥为$gpk_j=(g_1, g_2, \eta, u, v, w_j)$。类似的，为了实现不可否认性，群管理者依照ECDSA-160对信息(j, gpk_j)进行数字签名。

[0063] 网络运营商一旦接收到(j, gpk_j)后，将在他/她自己的本地记录中存储j和w_j之间的配对。最后，网络运营商将$\{g_1, g_2, \eta, u, v, h_0, h_1, h_2\}$和映射$(j, w_j)$发送给每个接入点。除此以外，网络运营商给每一个接入点(记为AP_k)赋予一个公/私钥对，表示为(PPK_k, PSK_k)。每一个接入点还获取了附带的由网络运营商数字签名的公钥证书，用于证实密钥的真实性。一个简单形式的证书由以下几部分组成：$Cert_k=\{AP_k, PPK_k, ExpT, SIG_{OSK}\{h(AP_k||PPK_k||ExpT)\}\}$。其中h(.)表示哈希函数操作，如SHA-1，ExpT是证书过期时间，$SIG_{OSK}\{h(AP_k||PPK_k||ExpT)\}$是网络运营商用其私钥OSK在$h(AP_k||PPK_k||ExpT)$上数字签名而生成的。

[0064] B.添加新用户阶段

[0065] 在接入网络之前，一个网络用户必须本人向群管理者联系进行认证。对每一个身

份为grp_j的用户群，一个身份为UID_i的用户i按如下步骤被赋予一个随机的成员密钥和群公钥：

[0066] 1.群管理者GM_j随机选择$x_i \in Z_p$，并用γ来计算$A_i = \frac{1}{x_i + \gamma} g_1$。$GM_j$在他/她的记录中存储对$(A_i, UID_i)$。

[0067] 2.群管理者GM_j通过一个安全传输协议(如有线传输层安全协议)向用户i传输信息$(j, gpk_j, msk[i])$。此时用户i的成员密钥为$msk[i]=(A_i, x_i)$。

[0068] 值得注意的是，在以上两步的环境中：

[0069] ●群管理者GM_j只保留成员密钥和用户身份信息的映射(A_i, UID_i)，而不保留群私钥gsk。

[0070] ●网络运营商只知道群私钥gsk而不知道映射(A_i, UID_i)。

[0071] 3.只有网络运营商知道映射(j, grp_j)。当然，每一个用户以及每个群管理者只能计算出他/她自己的群索引和群身份的映射。

[0072] C.撤销用户阶段

[0073] 用户群管理者GM_j一旦发现一些用户{1,...,r}已被攻破，将把这些被攻破用户视为需撤销的用户，并把撤销用户的列表$URL_J=\{A_1,...A_r\}$发送给网络运营商。接着，网络运营商在URL_J上数字签名并将其广播至每个接入点。

[0074] D.相互认证与密钥交换阶段

[0075] 一个网络用户i，若要接入网络，需要在一个接入点AP_k的直接通信范围内，并按照以下步骤进行相互认证与密钥交换：

[0076] 1.接入点AP_k选择一个随机数$r_P \in Z_p$并生成$r_P \cdot g_1$。接下来AP_k根据ECDSA-160对$r_P \cdot g_1$以及时间戳ts_1进行数字签名。然后，AP_k广播如下消息作为周期性地宣布其服务存在的信标消息：

[0077] $r_P \cdot g_1, ts_1, SIG_{PSK}\{r_P \cdot g_1 || ts_1\}, Cert_k$ (M1)

[0078] 2.用户i一旦收到(M1)，将执行如下操作：

[0079] a.检查时间戳ts_1的有效性以防止重放攻击。用OPK检查$Cert_k$来验证公钥的可靠性和AP_k的证书过期时间。然后通过PPK_k验证$SIG_{PSK}\{r_P \cdot g_1 || ts_1\}$。当且仅当它们都是有效的，才会执行下一步骤。

[0080] b.选择一个随机数$r_U \in Z_p$和一个临时的身份别名alias，然后计算$r_U \cdot g_1$。

[0081] c.在信息M上生成群签名σ。此时$M=\{alias, j, r_P \cdot g_1, r_U \cdot g_1, ts_2\}$。给定群公钥$gpk_j=(g_1, g_2, \eta, u, v, w_j)$，成员密钥$msk[i]=(A_i, x_i)$，和信息M，群签名σ可按照以下步骤计算：

[0082] -随机选择$\alpha, \beta \in Z_p$。

[0083] -计算A_i的加密和(T_1, T_2, T_3)，其中：

[0084] $T_1=\alpha u, T_2=\beta v, T_3=A_i+(\alpha+\beta)\eta$ (1)

[0085] -设置$\delta=\alpha x_i, \mu=\beta x_i$。

[0086] -随机选取盲值$r_\alpha, r_\beta, r_x, r_\delta, r_\mu \in Z_p$。设置

[0087] $R_1 = r_\alpha u, R_2 = r_\beta v, R_3 = \hat{e}(T_3, g_2)^{r_x} \hat{e}(\eta, (-r_\alpha - r_\beta) w_j + (-r_\delta - r_\mu) g_2), R_4 = r_x T_1 - r_\delta u, R_5 = r_x T_2 - r_\mu v$

[0088] -用以上的值和M计算得到c：

[0089] $c=H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$

[0090] -其中h(.)是一个输出结果范围为Z_p的哈希函数。

[0091] -设置:$s_\alpha=r_\alpha+c\alpha$,$s_\beta=r_\beta+c\beta$,$s_x=r_x+cx_i$,$s_\delta=r_\delta+c\delta$,$s_\mu=r_\mu+c\mu$。

[0092] -最后,合并以上求出的值形成群签名:

[0093] $\sigma=(T_1,T_2,T_3,c,s_\alpha,s_\beta,s_x,s_\delta,s_\mu)$

[0094] d.与AP_k生成共享的密钥:$SK_k=r_U \cdot (r_P \cdot g_1)$。

[0095] e.单播回复给AP_k

[0096] $alias,j,r_P \cdot g_1,r_U \cdot g_1,ts_2,\sigma$ (M2)

[0097] 值得注意的是用户i也可选择用AP_k的公钥PPK_k给信息{$alias,j,r_P \cdot g_1,r_U \cdot g_1,ts_2$}加密,然后在已加密信息上生成群签名σ。随后,用户i向AP_k单播已加密信息和群签名σ,而不是信息(M2)。很明显,在这种情况下,只有网络运营商和AP_k可以通过使用AP_k的私钥PSK_k来获取:

[0098] {$alias,j,r_P \cdot g_1,r_U \cdot g_1,ts_2$}

[0099] 3.在接收到信息(M2)后,AP_k进行以下步骤来认证用户i:

[0100] a.检查$r_P \cdot g_1$和ts_2的有效性以确保(M2)的新鲜性。

[0101] b.根据索引j选择群公钥gpk_j,然后进行群签名验证操作。首先重新计算挑战者c,然后根据以下步骤重构$(\tilde{R}_1,\tilde{R}_2,\tilde{R}_3,\tilde{R}_4,\tilde{R}_5)$:

[0102] -设置

[0103] $\tilde{R}_1=-cT_1+s_\alpha u,\tilde{R}_2=-cT_2+s_\beta v,\tilde{R}_3=\hat{e}(s_xT_3,g_2)\hat{e}(cT_3,w_j)\hat{e}(\eta,w_j)^{-s_\alpha-s_\beta}\cdot\hat{e}(\eta,g_2)^{-s_\delta-s_\mu}\hat{e}(g_1,g_2)^{-c}$

[0104] -设置$\tilde{R}_4=s_xT_1-s_\delta u,\tilde{R}_5=s_xT_2-s_\mu v$。

[0105] -当且仅当c等于$H(M,T_1,T_2,T_3,\tilde{R}_1,\tilde{R}_2,\tilde{R}_3,\tilde{R}_4,\tilde{R}_5)$时接受该信息。

[0106] c.根据索引j选择撤销用户列表URL_j,然后按如下步骤执行撤销检查:对于每个撤销标记$A_i \in URL_j$,AP_k检查A_i是否由σ的(T_1,T_2,T_3)编码而来。检查下面等式是否成立:

[0107] $\hat{e}(T_3-A_i,h_0)=\hat{e}(T_1,h_1)\hat{e}(T_2,h_2)$ (2)

[0108] 因为

[0109] $\hat{e}(T_3-A_i,h_0)=\hat{e}((\alpha+\beta)\eta,h_0)=\hat{e}(\alpha\cdot\eta+\beta\cdot\eta,h_0)$

[0110] $=\hat{e}(\alpha\cdot\eta,h_0)\hat{e}(\beta\cdot\eta,h_0)=\hat{e}(\alpha\cdot s_1\cdot u,h_0)\hat{e}(\beta\cdot s_2\cdot v,h_0)$

[0111] $=\hat{e}(\alpha\cdot u_1,s_1\cdot h_0)\hat{e}(\beta\cdot v,s_2\cdot h_0)=\hat{e}(T_1,h_1)\hat{e}(T_2,h_2)$,

[0112] 如果没有编码自(T_1,T_2,T_3)的URL撤销标记,则σ的签名者并未被撤销。

[0113] 如果所有以上的检查都成功,AP_k将会把接入请求视为有效和未经被授权用户改变的,并作出用户已建立了一个共享的对称密钥SK_k的结论。虽然AP_k不知道这究竟是哪一个用户。需要注意的是UID_i在协议运行的过程中是永远不会被泄露或传播的。

[0114] 4.AP_k利用$(r_U \cdot g_1,r_P)$信息,计算共享对称密钥$SK_k=r_P \cdot (r_U \cdot g_1)$并发送以下信息(M3)给用户i:

[0115] $alias,AP_k,r_U \cdot g_1,E_{SK_k}(AP_k,r_U \cdot g_1,r_P \cdot g_1)$ (M3)

[0116] 其中$E_K(X)$用对称密钥K加密了信息X。

[0117] 5.在接收了(M3)后,用户i解密并用对称密钥验证SK_k。如果(M3)是有效的,用户i

会认为AP_k已和他/她建立了一个共享密钥。否则，用户i会拒绝链接。以上协议不但使一个接入点与一个合法网络用户之间的显式相互认证可行，还使单边的用户匿名用户验证成为可能。一旦协议成功完成，接入点和用户之间会建立起一个共享对称密钥。这个密钥可用于往后的通信会话。这个会话是通过(alias,AP_k,$r_U \cdot g_1$)唯一标识的。

[0118] 验证一个接入点数字签名的计算开销主要由13个标量乘法(scalar multiplications，下同)和5个配对(pairing，下同)操作造成。显然，其中配对操作的计算开销远高于标量乘法操作的开销。

[0119] E.批量签名验证阶段

[0120] 计算R_3是验证过程中最耗费资源的部分。因为每个R_3都在验证等式中被哈希了，因此若不仔细思考较难看出这可以被批处理。设置$\sigma=(T_1,T_2,T_3,R_3,c,s_\alpha,s_\beta,s_x,s_\delta,s_\mu)$。也就是说，$R_3$作为σ的一部分被传输。在系统建立阶段，NO选择一个随机数$\varepsilon \in Z_p$，并把ε(作为群公钥的一部分)传输给每一个群管理者和每一个AP。设置

[0121] $$c = \varepsilon^{H(M,T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5)} \bmod p$$

[0122] 这里$\langle M^1,\sigma^1\rangle,\langle M^2,\sigma^2\rangle,\ldots,\langle M^n,\sigma^n\rangle$分别表示来自于同一用户群的n个不同用户$U_1,U_2,\ldots,U_n$标记为的接入请求信息。$AP_k$检查以下等式是否成立：$\prod_{i=1}^{n} c^i \bmod p = \varepsilon^{\sum_{i=1}^{n} H(M,T_1,T_2,T_3,\tilde{R}_1^i,\tilde{R}_2^i,R_3^i,\tilde{R}_4^i,\tilde{R}_5^i)} \bmod p$。如果这个等式成立，则$AP_k$检查以下等式是否成立：$\prod_{i=1}^{n} R_3^i = \prod_{i=1}^{n} \tilde{R}_3^i$。因此，对于这次检查，$AP_k$只需检查以下等式是否成立：

$$\prod_{i=1}^{n} R_3^i = \hat{e}(\sum_{i=1}^{n}(s_x^i T_3^i - c^i g_1 - (s_\delta^i + s_\mu^i)\eta), g_2)\hat{e}(\sum_{i=1}^{n} c^i T_3^i - (s_\alpha^i + s_\beta^i)\eta), w_j)。$$

[0123] 以上批验证等式是成立的，原因在于：

[0124] $$\prod_{i=1}^{n} \tilde{R}_3^i = \prod_{i=1}^{n} \hat{e}(s_x^i T_3^i, g_2)\hat{e}(c^i T_3^i, w_j)\cdot\hat{e}((-s_\alpha^i - s_\beta^i)\eta, w_j)\hat{e}((-s_\delta^i - s_\mu^i)\eta, g_2)\hat{e}((-c^i)g_1, g_2)$$

[0125]

$$= \hat{e}(\sum_{i=1}^{n} s_x^i T_3^i, g_2)\hat{e}(\sum_{i=1}^{n} c^i T_3^i, w_j)\cdot\hat{e}(\sum_{i=1}^{n}(-s_\alpha^i - s_\beta^i)\eta, w_j)\hat{e}(\sum_{i=1}^{n}(-s_\delta^i - s_\mu^i)\eta, g_2)\hat{e}(\sum_{i=1}^{n}(-c^i)g_1, g_2)$$

[0126] $$= \hat{e}(\sum_{i=1}^{n}(s_x^i T_3^i - c^i g_1 - (s_\delta^i + s_\mu^i)\eta, g_2)\hat{e}(\sum_{i=1}^{n}(c^i T_3^i - (s_\alpha^i + s_\beta^i)\eta), w_j)。$$

[0127] 所有签名$\sigma^1,\sigma^2,\ldots,\sigma^n$当且仅当以上两个检查都正确时才有效。在上述的批验证等式中，验证n个签名的计算消耗主要来自2个配对和13n个标量乘法操作。从而这极大地减少了验证大量签名所消耗的时间，同时也减少了由AP处签名验证这一潜在的瓶颈问题所导致的连接中断率。需注意的是所提出的方法继承了短群签名(SGS)技术的所有安全特性，此外，该方法还支持批验证。

[0128] 如果批验证返回一个负值，将会使用一个递归的“分而治之”方法。也就是说，简单地把集合分成两等份，然后对这两等份各自再进行验证。当这个过程结束时，AP输出每个无效签名的索引。这里设想：无效的包出现的几率是很小的。

[0129] F.用户追踪阶段

[0130] 当法律权威想追踪对特定通信会话负责的用户时，将进行以下几个步骤：

[0131] 1.网络运营商基于链接和会话标识，从网络日志文件中找到相应的会话认证信息(M2)。

[0132] 2.网络运营商把群签名σ的前三个元素(T_1,T_2,T_3)视为一个线性加密，并用群私钥(s_1,s_2)来获得用户的A_i，如等式(3)中所示。然后网络运营商向法律权威报告(A_i,j)。

[0133] $$A_i=T_3-(s_1 \cdot T_1+s_2 \cdot T_2) \qquad (3)$$

[0134] 因为：

[0135] $$T_3-(s_1 \cdot T_1+s_2 \cdot T_2)=A_i+(\alpha+\beta)\eta-(s_1 \cdot T_1+s_2 \cdot T_2)$$

[0136] $$=A_i+\alpha \cdot \eta+\beta \cdot \eta-s_1 \cdot \alpha \cdot u-s_2 \cdot \beta \cdot v=A_i$$

[0137] 法律权威向用户群管理者GM_j发送A_i。GM_j可以查看记录(A_i,UID_i)来找到对应的身份UID_i，然后把UID_i回复给法律权威。在这步上，只有法律权威可借助网络运营商和用户群管理者的帮助，在审查中确认需对特定通信会话负责的用户。

[0138] 有关的技术术语如下：

[0139] g_2表示G_2的随机生成元；

[0140] G_1表示循环加法群1；

[0141] G_2表示循环加法群2；

[0142] G_T表示与G_1和G_2拥有同样素数阶的循环乘法群；

[0143] ψ表示从G_2到G_1的同构映射；

[0144] gsk表示群私钥；

[0145] grp_i表示群管理者i的身份；

[0146] GM_j表示群管理者j；

[0147] Z_p表示小于或等于p的整数域；

[0148] (OPK,OSK)表示网络运营商数字签名使用的公/私钥对；

[0149] (PPK_k,PSK_k)表示网络运营商赋予每一个接入点的公/私钥对；

[0150] UID_i表示用户i的身份；

[0151] msk[i]表示成员i的成员密钥；

[0152] $\hat{e}$表示可计算的双线性映射$G_1 \times G_2 \rightarrow G_T$。

[0153] 上述实施例为本发明较佳的实施方式，但本发明的实施方式并不受上述实施例的限制，其他的任何未背离本发明的精神实质与原理下所作的改变、修饰、替代、组合、简化，均应为等效的置换方式，都包含在本发明的保护范围之内。

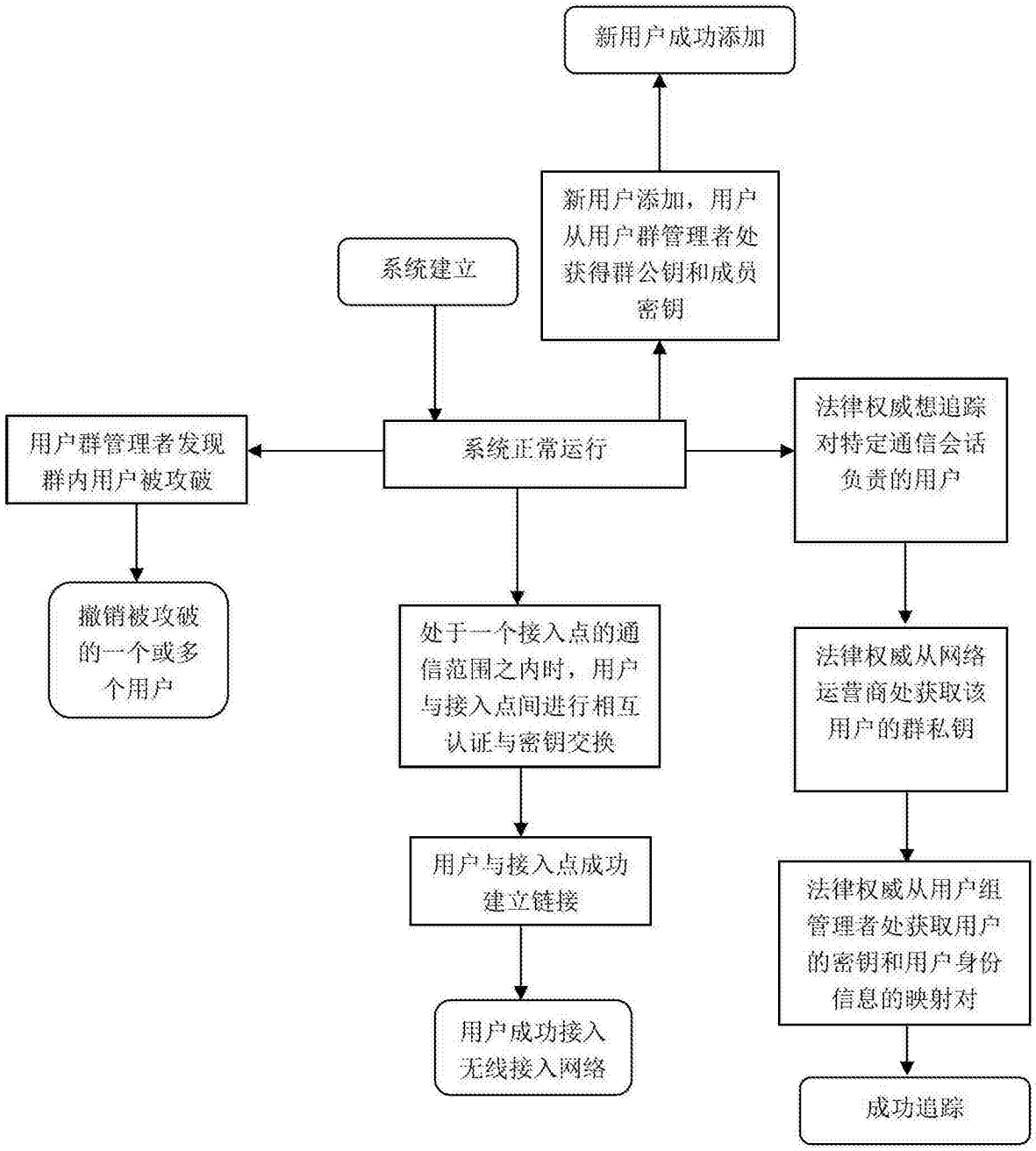

新用户成功添加
新用户添加，用户从用户群管理者处获得群公钥和成员密钥
系统建立
用户群管理者发现群内用户被攻破
系统正常运行
法律权威想追踪对特定通信会话负责的用户
撤销被攻破的一个或多个用户
处于一个接入点的通信范围之内时，用户与接入点间进行相互认证与密钥交换
法律权威从网络运营商处获取该用户的群私钥
用户与接入点成功建立链接
法律权威从用户组管理者处获取用户的密钥和用户身份信息的映射对
用户成功接入无线接入网络
成功追踪

图1

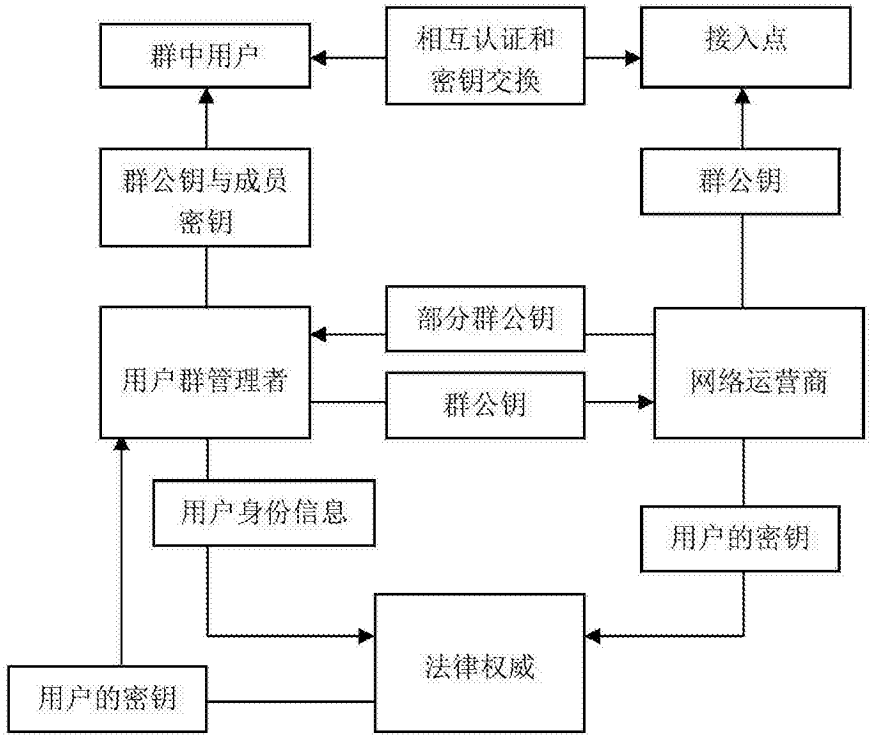

群中用户
相互认证和
密钥交换
接入点
群公钥与成员
密钥
群公钥
部分群公钥
用户群管理者
网络运营商
群公钥
用户身份信息
用户的密钥
法律权威
用户的密钥

图2