专 利 合 作 条 约

发信人：国际检索单位

收信人：

100004

中国北京市朝阳区建外大街 22 号赛特广场 7 层

北京集佳知识产权代理有限公司

逯长明

PCT

国际检索单位书面意见

(PCT 细则 43 之二 .1)

发文日 *(日/月/年)*	**26.2 月 2009 (26.02.2009)**
申请人或代理人的档案号	**后续行为**
0P080837	见下面第 2 段

国际申请号	国际申请日 *(日/月/年)*	优先权日 *(日/月/年)*
PCT/CN2008/073051	**14.11 月 2008(14.11.2008)**	16. 11 月 2007(16. 11. 2007)

国际专利分类(IPC)或国家分类和 IPC 两种分类

参见补充栏

申请人

西安西电捷通无线网络通信有限公司 等

1.本意见包括关于下列各项的内容：

- ☒ I 意见的基础
- ☒ II 优先权
- ☐ III 不作出关于新颖性、创造性和工业实用性的意见
- ☐ IV 缺乏发明的单一性
- ☒ V 按照细则 43 之二.1(a)(i)关于新颖性、创造性或工业实用性的理由；支持这种意见的引证和解释
- ☒ VI 引用的某些文件
- ☐ VII 国际申请中的某些缺陷
- ☐ VIII 对国际申请的某些意见

2. 后续行为

如果提出初步审查要求书，本次意见将被视为国际初步审查单位(IPEA)的一次书面意见（如果申请人选择的国际初步审查单位非本机构，而且所选国际初步审查单位已按照细则 66.1 之二(b)通知国际局将不考虑国际检索单位的书面意见时例外）。

如本书面意见被视为国际初步审查单位的书面意见，则请申请人在自 PCT/ISA/220 发文之日起 3 个月或自优先权日起 22 个月内（以后届满者为准）向国际初步审查单位提交书面答复并提交修改（如适用），

3. 详细信息请见 PCT/ISA/220 表格的说明

中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号： (86-10)62019451	完成本意见的日期 **16.2 月 2009 (16.02.2009)**	授权官员 韩燕 电话号码：(86-10) **62411765**

国际检索单位书面意见

国际申请号
PCT/CN2008/073051

I. 意见的基础

1、 关于语言，制定书面意见基于：

☒ 申请提出时使用的语言。

☐ 该申请的_____语言译文，为了国际检索的目的提供该种语言的译文(细则 12.3(a)和 23.1(b))。

2、☐ 该书面意见的制定考虑了该单位认可的根据细则 91 条所做出的明显错误更正（细则 43 之二 1（a））。

3、☐ 关于国际申请中所公开的**核苷酸和/或氨基酸序列表和对所称发明的必要性**，该书面意见是在下列基础上制定的：

a. 材料的类型

☐ 序列表

☐ 与序列表相关的表格

b. 材料的形式

☐ 纸件形式

☐ 电子形式

c. 提交/提供时间

☐ 包括于已提交的国际申请。

☐ 电子形式与国际申请一起提交。

☐ 为检索目的随后提交给本国际检索单位。

4、☐ 另外，在提交/提供了多个**核苷酸和/或氨基酸序列表和/或与其相关的表格的版本或副本的情况下，提供了关于后提交的或附加的副本与已提交的国际申请中的序列表相同或未超出国际申请中序列表范围（如适用）的声明。**

5. 补充意见

国际检索单位书面意见

国际申请号
PCT/CN2008/073051

II. 优先权

1. ☐ 没有考虑优先权的有效性，因为国际检索单位没有获得被要求优先权的在先申请的副本，或需要时该在先申请的译本。然而本意见是在假定所称优先权日是相关日的情况下作出的（细则 43 之二.1 和 64.1）。

2. ☒ 由于发现所要求的优先权是无效的，因此本意见是按照如同没有要求任何优先权的情况须做出的（细则 43 之二.1 和 64.1），因而，本意见中上面指明的国际申请日被认为是相关日。

3. 补充意见（如必要时）：

经核实，本申请所请求保护的技术方案中所记载的内容“认证器和请求者协商出一致的成对临时密钥 PTK”与本申请所要求的申请日为 2007 年 11 月 16 日（16.12.2007）、申请号为 200710019090.9 的优先权文本中记载的内容“认证器和请求者协商出一致的单播临时密钥 UTK”不一致，因此，本申请所要求的优先权不成立。

国际检索单位书面意见

国际申请号
PCT/CN2008/073051

V. 按细则 43 之二.1 关于新颖性、创造性或工业实用性的理由；支持这种意见的引证和解释

1. 意见

新颖性(N)　权利要求 1-4　是
权利要求 无　否

创造性(IS)　权利要求 无　是
权利要求 1-4　否

工业实用性(IA)　权利要求 1-4　是
权利要求 无　否

2. 引证和解释

(1) 参考以下文献：

D1: CN101159538A, 09.4 月 2008(09.04.2008)

D2: US20060107050A1, 18.5 月 2006(18.05.2006)

(2) D1 被认为是与权利要求 1 的主题最接近的现有技术。

D1 公开了一种密钥管理方法，并具体公开了如下技术特征（权利要求 1-6）：该方法为一种增强的 RSNA 的 4 步握手协议，其包括以下步骤：1）、认证器在消息（1）原有定义内容的基础上，添加密钥协商标识 KNID 和消息完整性码 MIC，构成新的消息（1）后，发送给请求者；2）、请求者收到新的消息（1）之后，验证其中的 MIC 字段是否正确，若不正确，则直接丢弃；否则，进行原有验证，若验证成功，则向认证器发送消息（2）；3）、认证器收到消息（2）之后，进行原有验证，若验证成功，则向请求者发送消息（3）；4）、请求者收到消息（3）之后，进行原有验证，若验证成功，则向认证器发送消息（4）；5）、认证器收到消息（4）之后，进行原有验证，若验证成功，则 4 步握手协议成功完成，认证器和请求者协商出一致的单播临时密钥 UTK，并各自得到对方的组播主密钥 GMK。所述消息（1）原有定义内容以及消息（2）、消息（3）和消息（4）的内容分别与 IEEE 802.11i-2004 标准文本中的定义相同。所述原有验证均为 802.11i-2004 标准文本中的验证过程。权利要求 1 与 D1 的区别技术特征在于：权利要求 1 包括认证器和请求者协商出一致的成对临时密钥 PTK。因此权利要求 1 具备 PCT 条约第 33 条(2)规定的新颖性。由此确定权利要求 1 的技术方案解决的技术问题为：认证器和请求者协商出一致的成对临时密钥 PTK。该区别技术特征被 D2 公开了（说明书第[0018]段）：认证器 110 还将 ANonce、Snonce、其自己的 PMK 以及其他相关值带入由请求者 120 使用的同一方程以便产生 PTK，利用 PTK 中的 PCK 计算 EAPOL-Key2 的 MIC，并且将计算出的值与 EAPOL-Key2 中的 MIC 值进行比较。如果请求者 120 与认证器 110 持有相同的 PMK，则由双方所产生的 MIC 应当也是相同的。在完成后面的 EAPOL-Key3 和 EAPOL-Key4 交换之后，认证器 110 和请求者 120 将安装所产生的 PTK。D1 和 D2 都涉及密钥管理协议，因此本领域技术人员在 D1 和 D2 的基础上得到权利要求 1 的技术方案是显而易见的，因此权利要求 1 不具备 PCT 条约第 33 条(3)规定的创造性。

权利要求 2 是权利要求 1 的从属权利要求，因此权利要求 2 具备 PCT 条约第 33 条(2)规定的新颖性。权利要求 2 的附加技术特征已经被 D1（权利要求 2）公开了：所述步骤 1）中消息完整性码 MIC 为认证器利用认证阶段已协商的成对主密钥 PMK 对 MIC 字段之前的所有字段计算的杂凑值。因此，本领域技术人员在 D1 和 D2 的基础上得到权利要求 2 的技术方案是显而易见的，因此权利要求 2 不具备 PCT 条约第 33 条(3)规定的创造性。

权利要求 3 是权利要求 1 的从属权利要求，因此权利要求 3 具备 PCT 条约第 33 条(2)规定的新颖性。权利要求 3 的附加技术特征已经被 D1（权利要求 3）公开了：所述步骤 1）中的密钥协商标识 KNID，若此次过程为 RSNA 认证成功后的首次 4 步握手协议，则其为认证器产生的随机数，若为密钥更新过程，则其为上一次 4 步握手协议成功后，认证器根据成对主密钥 PMK、NonceA、NonceS 计算得到的值。因此，本领域技术人员在 D1 和 D2 的基础上得到权利要求 3 的技术方案是显而易见的，因此权利要求 3 不具备 PCT 条约第 33 条(3)规定的创造性。

权利要求 4 是权利要求 1、2 或 3 的从属权利要求，因此权利要求 4 具备 PCT 条约第 33 条(2)规定的新颖性。权利要求 4 的附加技术特征“验证 KNID 是否正确”已经被 D1（权利要求 4）公开了：若为密钥更新过程，所述步骤 2）中请求者还要验证 KNID 是否正确，不正确，则直接丢弃。而 MIC 的验证已经在 D1 的权利要求 1 中公开了（如上所述）。因此，本领域技术人员在 D1 和 D2 的基础上得到权利要求 4 的技术方案是显而易见的，因此权利要求 4 不具备 PCT 条约第 33 条(3)规定的创造性。

国际检索单位书面意见

国际申请号
PCT/CN2008/073051

VI. 某些引用文件

1. 某些已公布的文件(细则 43 之二.1 和 70.10)

申请号 专利号	公布日 *(日/月/年)*	申请日 *(日/月/年)*	优先权日(有效的) *(日/月/年)*
200710019090.9	09/04/2008	16/11/2007	

2. 非书面公开(细则 43 之二.1 和 70.9)

非书面公开的种类	非书面公开的日期 *(日/月/年)*	述及非书面公开的 书面公开的日期 *(日/月/年)*

补充栏
(当前面的任何一栏篇幅不够时使用本栏)

续　　栏：

续扉页
国际专利分类(IPC)或国家分类和 IPC 两种分类
H04L9/00(2006.01)i
H04L29/06(2006.01)n
H04L12/28(2006.01)n

续第 V 栏
引证和解释

（3） 权利要求 1-4 要求保护的技术方案可以在工业上制造或使用，因此，权利要求 1-4 具备工业实用性，符合 PCT 条约第 33 条(4)的规定。