WAPI 密钥管理协议的 PCL 证明

铁满霞 李建东 王育民
(西安电子科技大学 ISN 国家重点实验室 西安 710071)
(西安电子科技大学信息科学研究所 西安 710071)

摘 要：该文利用协议合成逻辑(PCL)，对 WAPI 密钥管理协议进行了模块化正确性证明。首先，分析了相对独立的单播密钥协商与组播密钥通告协议，在满足一定的工作环境下，证明其分别具有 SSA 与 KS 特性，且与协议的实体与会话个数无关；接着，根据顺序合成规则与阶段合成定理，由于参与协议运行的实体避免了基于同一 BK 担当 AE 和 ASUE 两种角色，且每个子协议的运行都不干扰或不破坏其他子协议的环境条件，故 WAPI 密钥管理协议具有所需的安全属性，达到协议设计目标。

关键词：无线局域网；无线局域网鉴别与保密基础结构；密钥管理协议；协议合成逻辑；安全性证明
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2009)02-0444-04

A Correctness Proof of WAPI Key Management Protocol Based on PCL

Tie Man-xia Li Jian-dong Wang Yu-min
(*State Key Laboratory of Integrated Services Networks*, *Xidian University*, *Xi'an* 710071,*China*)
(*Information Science Institute*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: Based on PCL, a formal correctness proof of WAPI key management protocol is presented. First, unicast key negotiation and multicast key announcement sub-protocols are analyzed, and their separate proofs of specific security properties of SSA and KS are detailed under unbounded number of participants and sessions. Second, according to the sequential rule and staged composition theorem, all principals do not execute both roles of ASUE and AE, and the precondition of a sub-protocol is preserved by the other one later in the chain, so, WAPI key management protocol possesses the required security properties and achieves its predefined goals.

Key words: WLAN; WLAN Authentication and Privacy Infrastructure(WAPI); Key management protocol; Protocol Composition Logic (PCL); Security proof

1 引言

为了解决无线局域网 (Wireless Local Area Network, WLAN)国际标准 ISO/IEC 8802-11 中定义的 WEP(Wired Equivalent Privacy)安全机制存在的安全漏洞，我国分别于 2003 年与 2006 年颁布了无线局域网国家标准及其第一号修改单[1,2]，采用无线局域网鉴别与保密基础结构 (WLAN Authentication and Privacy Infrastructure, WAPI)安全机制解决无线局域网的安全问题。WAPI 密钥管理协议包含单播密钥协商与组播密钥通告两个相对独立的子过程，参与的实体有鉴别请求者实体 (Authentication Supplicant Entity, ASUE)和鉴别器实体(Authenticator Entity, AE)，基于证书鉴别结果或预共享密钥或缓存的基密钥 (Base Key, BK)，实现数据通信会话可用密钥的协商与分发。

安全协议的分析与证明对于现代安全网络系统至关重要，通常利用模型检测方法(如 Murφ 模型[3,4]与有限状态(finite-state)[5]等)查找协议错误，采用逻辑(如 BAN)和理论证明方法证实协议的正确性。模型检测方法一般仅考虑有限个协议会话同时进行，逻辑和理论证明方法所提供的安全性与协议会话的个数无关。协议合成逻辑 (Protocol Composition Logic, PCL)[6−10]是一种用于证明网络协议安全性能的逻辑，相比其它的逻辑方法如 BAN 逻辑，主要特征有：由于包含了协议的执行过程，不需要对协议进行抽象；采用标准逻辑概念，避免使用裁判权(jurisdiction)和信任(belief)等不清晰规则，直接与协议的执行语义相关联；支持安全协议的合成推导，这些协议可以并列合成，也可顺序合成。PCL 逻辑目前已被成功用于验证数个协议的正确性，如 Datta 等[10]将此逻辑应用于 ISO-9798-3 所定义的协议中，He 等[11]还利用其成功证明了 IEEE 802.11i 协议的正确性。本文将利用 PCL 逻辑，采用相似方法，给出 WAPI 密钥管理协议的正确性证明。

2007-08-23 收到，2008-02-18 改回
国家杰出青年科学基金(60725105)，国家自然科学基金重大项目(60496316)，国家 863 计划项目(2007AA01Z217)和国家自然科学基金(60572146)资助课题

2 PCL 逻辑

2.1 协议逻辑

协议执行时涉及若干实体，每个实体在执行协议的过程

中可以包含若干实例。实体记为 $\widehat{X}$，实例记为 X，遵循规则 $\theta[P]_X\phi$，该规则表明实例 X 执行 P 行为后，状态由 θ 转换为 ϕ。PCL 定义了许多谓词(predicate)，用于断言实体已执行的确定行为。本文用到的谓词如下：

Has(X,x)：秘密属性的一种描述，表示实体 $\widehat{X}$ 在实例 X 中拥有信息 x，该信息 x 可以是本地产生，或者明文收到，或者已知解密密钥的前提下收到的加密数据；

Send(X,m)：表示实体 $\widehat{X}$ 在实例 X 中已发送消息 m；

Receive(X,m)，New(X,t)，Decrypt(X,t) 意味着已发生了接收(receive)、产生随机数(new)及解密(decrypt)行为。

Fresh(X,t)：表示在实例 X 中产生的 t 是新鲜的；

Honest($\widehat{X}$)：表示实体 $\widehat{X}$ 在当前轮中是诚实的，其执行的所有行为都是协议所规定的；

Start(X)：表示实例 X 过去从未执行任何行为。

2.2 证明系统

a 表示任意一种 send，receive，new 及 decrypt 等的行为，α 表示与逻辑中这些行为相对应的谓词。

AA1　$\phi[a]_X\alpha$；

AA4　$\phi[a_1;a_2;\cdots;a_k]_X\alpha_1<\alpha_2\wedge\cdots\wedge\alpha_{k-1}<\alpha_k$；

AN3　$\phi[\text{new}\ \ x]_X\text{Fresh}(X,x)$；

ARP　$\text{Receive}(X,p(x))[\text{match}\ q(x)/q(t)]_X\ \text{Receive}(X,p(t))$；

P1　$\text{Persist}(X,t)[a]_X\text{Persist}(X,t)$；

FS1　$\text{Fresh}(X,t)[\text{send}\ t']_X\text{FirstSend}(X,t,t')$，其中 $t\subseteq t'$；

HON　$\dfrac{\text{Start}(X)[\ ]_X\phi\quad\forall\rho\in\vartheta.\forall P\in\text{BS}(\rho).\phi[P]_X\phi}{\text{Honest}(\widehat{X})\supset\phi}$；

HASH1　$\text{Compute}(X,\text{HASH}_K(x))\supset\text{Has}(X,x)\wedge\text{Has}(X,K)$；

HASH3　$\text{Receive}(X,\text{HASH}_K(x))\supset\exists A.\text{Compute}(A,\text{HASH}_K(x))\wedge\text{Send}(A,\text{HASH}_K(x))$；

HASH4　$\text{Has}(X,\text{HASH}_K(x))\supset\text{Compute}(X,\text{HASH}_K(x))\vee\exists A,m.\text{Compute}(A,\text{HASH}_K(x))\wedge\text{Send}(A,m)\wedge\text{Contain}(m,\text{HASH}_K(x))$;

S1　$\dfrac{\phi_1[P]_X\phi_2\quad\phi_2[P']_X\phi_3}{\phi_1[PP']_X\phi_3}$。

3　WAPI 单播密钥协商协议

WAPI 单播密钥协商协议通过单播密钥协商请求、响应与确认的 3 步消息交互，产生用于保护单播数据和组播密钥的单播会话密钥 USK(Unicast Session Key)。

3.1 协议模型

WAPI 单播密钥协商协议的参与实体有 AE 和 ASUE，分别用 $\widehat{X}$，$\widehat{Y}$ 表示，各自相应实例用 X，Y 表示。该协议运行时，假设两个实体已具有共享的基密钥 BK 且不被第三方知晓，即 $\theta_{\text{WAPIU}}:=\text{Honest}(\widehat{X})\wedge\text{Honest}(\widehat{Y})\supset\left(\text{Has}\left(\widehat{A},\text{BK}\right)\supset\widehat{A}=\widehat{X}\vee\widehat{A}=\widehat{Y}\right)$。该协议表述如下：

WAPIU:AE = $(X,\widehat{Y},\text{BK})[$
　new x; send $\widehat{X},\widehat{Y},\text{msgID1},x$; receive $\widehat{Y},\widehat{X},\text{msg2}$;
　match msg2/msgID2,x,y,hmac1;
　match $\text{HASH}_{\text{BK}}(x,y)/\text{USK}$;
　match hmac1/HASH_{USK}(msg2);
　send $\widehat{X},\widehat{Y},\text{msgID3},\ x,y,\text{HASH}_{\text{USK}}(\text{msg3})]_X$。

WAPIU:ASUE = $(Y,\text{BK})[$
　receive $\widehat{X},\widehat{Y},\text{msg1}$; match msg1/msgID1,$x$; new y;
　match $\text{HASH}_{\text{BK}}(x,y)/\text{USK}$;
　send $\widehat{Y},\widehat{X},\text{msgID2},x,y,\ \text{HASH}_{\text{USK}}(\text{msg2})$;
　receive $\widehat{X},\widehat{Y},\text{msg3}$; match msg3/msgID3,$x,y$,hmac2;
　match hmac2/$\text{HASH}_{\text{USK}}(\text{msg3})]_Y$。

3.2 工作环境

$\Gamma_{\text{WAPIU},1}:=\text{Compute}(\widehat{X},\text{HASH}_{\text{BK}}(x,y))\supset\neg(\text{Send}(\widehat{X},m)\wedge\text{Contain}(m,\text{HASH}_{\text{BK}}(x,y)))$;

$\Gamma_{\text{WAPIU},2}:=(\text{Honest}(\widehat{X})\wedge\text{Receive}(X,\text{msg1})\supset\neg\text{Send}(X,\text{msg3}))\wedge(\text{Honest}(\widehat{X})\wedge\text{Send}(X,\text{msg1})\supset\neg\text{Send}(X,\text{msg2}))$。

在 WAPI 单播密钥协商协议运行过程中，$\Gamma_{\text{WAPIU},1}$ 描述 AE 和 ASUE 根据 x，y 与 BK 本地推演的 USK 不能泄露给第三方；$\Gamma_{\text{WAPIU},2}$ 表述同一网元不能同时即作为 AE 又作为 ASUE，同时兼任两个角色会引起反射攻击[4]。

3.3 安全属性及证明

WAPI 单播密钥协商协议的安全目标可形式化表示为强壮的会话鉴别 SSA(Strong Session Authentication)和密钥秘密 KS(Key Secrecy)安全属性，且只有保障 KS 特性，才能确保具有 SSA 属性。AE 和 ASUE 通过单播密钥协商形成匹配会话，这里仅给出 AE 端的情况，ASUE 端的情况类似，略去。

定理 1　WAPI 单播密钥协商协议为 AE 提供 KS 属性 $\Gamma_{\text{WAPIU},1}\wedge\Gamma_{\text{WAPIU},2}\mapsto\ \theta_{\text{WAPIU}}[\text{WAPIU:AE}]_X\phi_{\text{WAPIU,sec}}$，其中 $\phi_{\text{WAPIU,sec}}::=\text{Honest}(\widehat{X})\wedge\text{Honest}(\widehat{Y})\supset\text{Has}(\widehat{X},\text{USK})\wedge\text{Has}(\widehat{Y},\text{USK})\supset(\text{Has}(\widehat{A},\text{USK})\supset(\widehat{A}=\widehat{X}\vee\widehat{A}=\widehat{Y}))$。

证明

ARP,HASH3　$\theta_{\text{WAPIU}}[\text{receive}\ \ \widehat{Y},\widehat{X},\text{msg2};$
match msg2/msgID2,x,y,hmac1;
match $\text{HASH}_{\text{BK}}(x,y)/\text{USK}$;
match hmac1/HASH_{USK}(msg2);$]_X$
$\text{Receive}(X,(\widehat{Y},\widehat{X},\text{msg2}))\supset\exists A.\text{Compute}(A,\text{HASH}_{\text{USK}}(\text{msg2}))\wedge\text{Send}(A,\text{HASH}_{\text{USK}}(\text{msg2}))\wedge(\text{Send}(A,\text{HASH}_{\text{USK}}(\text{msg2}))<\text{Receive}(X,(\widehat{Y},\widehat{X},\text{msg2})))$　(1)

HASH1 $\text{Compute}(A,\text{HASH}_{\text{USK}}(\text{msg2}))\supset \text{Has}(A,\text{USK})\wedge\text{Has}(A,\text{msg2})$ (2)

HASH4 $\text{Has}(A,\text{USK})\equiv\text{Has}(A,\text{HASH}_{\text{BK}}(x,y))\supset \text{Compute}(A,\text{HASH}_{\text{BK}}(x,y))\vee(\exists B,m.\text{Compute}(B,\text{HASH}_{\text{BK}}(x,y))\wedge\text{Send}(B,m)\wedge\text{Contain}(m,\text{HASH}_{\text{BK}}(x,y)))$ (3)

$3,\Gamma_{\text{WAPIU,1}}$ $\theta_{\text{WAPIU}}[\text{WAPIU:AE}]_X \text{Has}(A,\text{USK})\equiv\text{Has}(A,\text{HASH}_{\text{BK}}(x,y))\supset\text{Compute}(A,\text{HASH}_{\text{BK}}(x,y))$ (4)

$4,\theta_{\text{WAPIU}}$,HASH1 $\theta_{\text{WAPIU}}[\text{receive}\ \widehat{Y},\widehat{X},\text{msg2};$ match msg2/msgID2,x,y,hmac1; match $\text{HASH}_{\text{BK}}(x,y)$ / USK; match hmac1/$\text{HASH}_{\text{USK}}(\text{msg2});]_X$ $\text{Honest}(\widehat{X})\wedge\text{Honest}(\widehat{Y})\supset \text{Compute}\ (A,\text{HASH}_{\text{BK}}(x,y))\supset\text{Has}(\widehat{A},\text{USK})\supset(\text{Has}(\widehat{A},\text{BK})\supset\widehat{A}=\widehat{X}\vee\widehat{A}=\widehat{Y})$ (5)

即 $\Gamma_{\text{WAPIU,1}}\wedge\Gamma_{\text{WAPIU,2}}\mapsto\theta_{\text{WAPIU}}[\text{WAPIU:AE}]_X\phi_{\text{WAPIU,sec}}$ 成立。

定理 2 WAPI 单播密钥协商协议为 AE 提供 SSA 属性 $\Gamma_{\text{WAPIU,1}}\wedge\Gamma_{\text{WAPIU,2}}\mapsto\ \theta_{\text{WAPIU}}[\text{WAPIU:AE}]_X\phi_{\text{WAPIU,auth}}$，其中 $\phi_{\text{WAPIU,auth}}::=\text{Honest}(\widehat{X})\wedge\text{Honest}(\widehat{Y})\supset\ \exists X.\text{Actions InOrder}(\text{Send}(X,(\widehat{X},\widehat{Y},\text{msg1})),\text{Receive}(Y,(\widehat{Y},\widehat{X},\text{msg1})),\text{Send}(Y,(\widehat{Y},\widehat{X},\text{msg2})),\text{Receive}(X,(\widehat{Y},\widehat{X},\text{msg2})),\ \text{Send}(X,(\widehat{X},\widehat{Y},\text{msg3})),\text{Receive}(Y,(\widehat{X},\widehat{Y},\text{msg3})))$。

证明 由于篇幅限制，这里的详细证明过程省略。

4 WAPI 组播密钥通告协议

WAPI 组播密钥通告协议利用组播密钥通告与响应两步消息交互，通告用于保护组播数据的组播会话密钥 MSK (Multicast Session Key)。

4.1 协议模型

WAPI 组播密钥通告协议运行时，单播密钥协商过程已成功结束，且 AE 和 ASUE 实体已具有单播会话密钥 USK 且不被第三方知晓，即 $\theta_{\text{WAPIM}}::=\text{Honest}(\widehat{X})\wedge\text{Honest}(\widehat{Y})\supset(\text{Has}(\widehat{A},\text{USK})\supset\widehat{A}=\widehat{X}\wedge\widehat{A}=\widehat{Y})$。协议表述如下：

WAPIM:AE = $(X,\widehat{Y},\text{SeqNo,USK,MSK})[$
match SeqNo/NewDSeqNo;
send $\widehat{X},\widehat{Y}$,msgID4,NewSeqNo,ENC_{USK}(MSK), HASH_{USK}(msg4); receive $\widehat{Y},\widehat{X}$,msg5;
match mag5/msgID5,SeqNo, hmac4;
match hmac4/$\text{HASH}_{\text{USK}}(\text{msg5})]_X$

WAPIM:ASUE = (Y,USK,OldSeqNo)[
receive $\widehat{X},\widehat{Y}$,msg4; match msg4/msgID4, NewSeqNo,ENC_{USK}(MSK),hmac3;
match hmac3/HASH_{USK}(msg4);
isLess OldSeqNo,NewSeqNo;
send $\widehat{Y},\widehat{X}$,msgID5,NewSeqNo,$\text{HASH}_{\text{USK}}(\text{msg5})]_Y$

4.2 工作环境

$\Gamma_{\text{WAPIM,1}}::=(\text{Honest}(\widehat{Y})\supset\neg(\exists Y,m.\text{Decrypt}(Y,(\text{MSK}))\wedge\text{Send}(Y,m)\wedge\text{Contain}(m,\text{MSK}))\wedge(\text{Honest}(\widehat{X})\supset\neg(\text{Send}(\widehat{X},m)\wedge\text{Contain}(m,\text{MSK})))$

$\Gamma_{\text{WAPIM,2}}::=\text{Honest}(\widehat{X})\wedge\text{Send}(X,\text{msg4})\supset\neg\text{Send}(X,\text{msg5})$

在 WAPI 组播密钥通告协议运行中，$\Gamma_{\text{WAPIM,1}}$ 描述 AE 和 ASUE 均不能将 USK 泄露给第三方；$\Gamma_{\text{WAPIM,2}}$ 表述一个网元不能同时既作为 AE 又作为 ASUE，否则与单播密钥协商协议相似，将引起反射攻击。

4.3 安全属性

定理 3 WAPI 组播密钥通告协议为 AE 提供 KS 属性 $\Gamma_{\text{WAPIM,1}}\wedge\Gamma_{\text{WAPIM,2}}\mapsto\ \theta_{\text{WAPIM}}[\text{WAPIM:AE}]_X\phi_{\text{WAPIM,sec}}$，其中 $\phi_{\text{WAPIM,sec}}::=\text{Honest}(\widehat{Y}_1)\wedge\text{Honest}(\widehat{Y}_2)\wedge\cdots\wedge\text{Honest}(\widehat{Y}_n)\supset(\text{Has}(\widehat{A},\text{MSK})\wedge\widehat{A}\neq\hat{X}\supset\widehat{A}=\widehat{Y}_1\vee\widehat{A}=\widehat{Y}_2\vee\cdots\widehat{A}=\widehat{Y}_n)$。

定理 4 WAPI 组播密钥通告协议为 AE 提供密钥有序 KO(Key Ordering) 属性 $\Gamma_{\text{WAPIM,1}}\wedge\Gamma_{\text{WAPIM,2}}\mapsto\theta_{\text{WAPIM}}[\text{WAPIM:AE}]_X\phi_{\text{WAPIM,ord}}$，其中 $\phi_{\text{WAPIM,ord}}::=\text{Honest}(\widehat{X})\supset(\text{Send}(X,(\widehat{X},\widehat{Y},\text{msgID4,SeqNo1,ENC}_{\text{USK}}(\text{MSK1}),\text{HASH}_{\text{USK}}(\text{msg4})))\wedge\ \text{Send}(X,(\widehat{X},\widehat{Y},\text{msgID4,SeqNo2,ENC}_{\text{USK}}(\text{MSK2}),\ \text{HASH}_{\text{USK}}(\text{msg4})))\wedge\ \text{isLess}(\text{SeqNo1,SeqNo2})\supset\ \text{FirstSend}(X,(\widehat{X},\widehat{Y},\text{msgID4,SeqNo1,ENC}_{\text{USK}}(\text{MSK1}),\ \text{HASH}_{\text{USK}}(\text{msg4})))\wedge\ \text{FirstSend}(X,(\widehat{X},\widehat{Y},\text{msgID4,SeqNo2,ENC}_{\text{USK}}(\text{MSK2}),\text{HASH}_{\text{USK}}(\text{msg4}))))$。

5 协议合成

根据文献[11]定义的阶段合成定理 SCT(Staged Composition Theorem)：给定子协议 $Q_1,Q_2,\cdots,Q_n$，若 (i) $\forall i,\Gamma_i\mapsto\theta_i[P_i]_X\phi_i$；(ii) $\forall i,j,Q_i\mapsto\Gamma_j$；(iii) $\forall i,\phi_i\supset\theta_{i+1}$；(iv) $\forall B\in\bigcup_{j\geq i}\text{ProtocolSteps}(Q_j),\theta_i[B]_X\theta_i$，则有 $\text{SCT}(<Q_1,Q_2,\cdots,Q_n>)\mapsto\theta_1[P;P_i]_X\phi_i$ 其中 $P;P_i\in\text{SCT}(<Q_1,Q_2,\cdots,$ 且 $P_i\in Q_i$。

WAPI 单播密钥协商与组播密钥通告协议的安全属性分别由定理 1，定理 2，定理 3 及定理 4 描述，每个子协议都充分考虑与保证其他子协议运行时所依赖的工作环境，且单播密钥协商协议的后向条件为组播密钥通告协议的先决条件，即 $\phi_{\text{WAPIU}}\supset\theta_{\text{WAPIM}}$，因此由规则 S1 和 SCT 有：当运行 WAPI 协议时，同一网元避免了基于相同 BK 担任 AE

和 ASUE，则 WAPI 密钥管理协议具有定理 1 至定理 4 所述的安全属性，且与单个协议的错误(超时、分组无效等)处理机制无关。

6　结束语

本文利用 PCL 逻辑，给出了 WAPI 密钥管理协议的模块化正确性证明，所依赖的工作条件可为协议的具体实现与网络部署提供保障与指导。

参 考 文 献

[1] 黄振海, 郭宏, 王育民等. GB 15629.11-2003《信息技术 系统间远程通信和信息交换局域网和城域网特定要求第 11 部分: 无线局域网媒体访问控制和物理层规范》. 北京, 中国标准出版社, 2003.

Huang Z H, Guo H, and Wang Y M *et al*.. GB15629.11, Information technology-Telecommunication and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Standards Press of China, 2003.

[2] 赖晓龙, 曹军, 铁满霞等. GB 15629.11-2003/XG1-2006《信息技术系统间远程通信和信息交换局域网和城域网特定要求第 11 部分: 无线局域网媒体访问控制和物理层规范第 1 号修改单》, 北京: 中国标准出版社, 2006 年.

Lai X L, Cao J, and Tie M X, *et al*.. GB15629.11-2003/XG1-2006, Information technology- Telecommunication and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11:Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 1, Beijing: Standards Press of China, 2006.

[3] Cremers C. On the Protocol Composition Logic PCL. http://arxiv.org/abs/0709.1080v4, 2007.

[4] 铁满霞, 李建东, 张变玲等. 一种适用于IBSS网络的无线接入认证协议. 电子与信息学报, 2008, 30(1): 6–9.

Tie M X, Li J D, and Zhang B L, *et al*.. A wireless access authentication protocol suitable for IBSS networks. *Journal of Electronics & Information Technology*, 2008, 30(1): 6–9.

[5] Mitchell J C, Shmatikov V, and Stern U. Finite-state analysis of ssl 3.0. Proceedings of the Seventh USENIX Security Symposium, San Antonio, 1998: 201–216.

[6] Datta A, Derek A, and Mitchell J C, *et al*.. A derivation system for security protocols and its logical formalization. Proceedings of 16th IEEE Computer Security Foundations Workshop, Asilomar, 2003: 109–125.

[7] Datta A, Derek A, and Mitchell J C, *et al*.. A derivation system and compositional logic for security protocols. *Journal of Computer Security*, 2005, 13(3): 423–482.

[8] Derek A. Formal analysis of security protocols: Protocol composition logic. [Ph.D. dissertation], Computer Science Department, Stanford University, December 2006.

[9] Durgin N, Mitchell J C, and Pavlovic D. A compositional logic for proving security properties of protocols. *Journal of Computer Security*, 2003, 11(4): 677–721.

[10] Datta A, Derek A, Mitchell J C and Roy A. Protocol Composition Logic (PCL). http://www.stanford.edu/~danupam/ddmr-pcl06.pdf, 2006.

[11] He C H, Sundararajan M, and Datta A, *et al*.. A modular correctness proof of IEEE 802.11i and TLS. Proceedings of 12th ACM Conference on Computer and Communications Security, Alexandria, 2005: 2–15.

铁满霞：　女，1968 年生，副教授，博士生，研究方向为宽带无线 IP 技术、移动通信、信息安全等.

李建东：　男，1962 年生，教授，博士生导师，博士，研究方向为宽带无线 IP 技术、移动通信、软件无线电、Ad hoc 自组织网络等.

王育民：　男，1936 年生，教授，博士生导师，研究方向为信息论、编码、密码等.