数字移动通信系统中认证协议的设计与分析

王全来[①②] 韩继红[①] 王亚弟[①]
[①](解放军信息工程大学电子技术学院 郑州 450004)
[②](解放军防空兵指挥学院 郑州 450052)

摘 要：该文针对数字移动通信系统的背景和需求，基于公钥密码体制设计了一个端端密钥分发协议，基于对称密码体制设计了一个身份认证协议，并利用 Spi 演算对身份认证协议进行了分析，证明了其安全性。

关键词：查询系统；认证协议；Spi 演
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2007)01-0189-04

Design and Analysis of an Authentication Protocol for Digital Mobile Communication System

Wang Quan-lai[①②] Han Ji-hong[①] Wang Ya-di[①]
[①](*Institute of Electronic Technology, the PLA University of Information Engineering, Zhengzhou* 450004, *China*)
[②](*Air Defense Forces Command College, Zhengzhou* 450052, *China*)

Abstract: This paper designs a communion key distribution protocol based on asymmetric cipher system, and an authentication protocol based on symmetric cipher system for the requirement of digital mobile communication system. Then this protocol is analyzed by using the Spi calculus and its security is proved.

Key words: Network-inquiry system; Authentication protocol; Spi calculus

1 引言

随着移动用户对信息服务的需求越来越多，对移动通信系统安全的要求也越来越高，这不仅包括数据通信的安全性，还要求身份认证的合法性。身份认证的安全性对整个通信安全具有十分重要的作用。目前实现身份认证最可行最安全的方式是设计基于密码技术的身份认证协议，并将其运用于认证系统中[1]。目前数字移动通信常使用的认证协议有 MSR 认证协议、Beller-Yacobi 认证协议、Aziz-Diffie 认证协议、TMN 协议等，通过分析这些协议，其不足在于对移动用户的计算能力考虑得较少，消息的新鲜性没有得到保证，易于遭受重放攻击与中间人攻击等攻击[2−5]。本文基于对称密码体制设计了一个身份认证协议，与现有的认证协议相比，所设计的新认证协议一个显著的特点是基于公钥密码体制设计了一个端端密钥分发协议，然后在此基础上基于对称密码体制设计了一个身份认证协议。这样设计的优点在于既完成了移动用户与应用服务器之间的双向认证，又通过利用一次性公钥证书保证了消息的新鲜性。

通信时，数字移动终端(C)向应用服务器 AS 查询秘密信息，AS 验证移动终端 C 的身份后，将信息加密传给数字移动终端。由于对数字移动终端的身份认证和消息的加密需要进行密码操作，因此在应用服务器 AS 后端建立密码服务代理。该代理与 AS 之间以专用接口协议进行通信，所有移动终端查询的身份认证和加解密操作都在密码服务代理中进行，对用户是透明的。基于此，我们在协议描述中将 AS 和密码服务代理看成是一个实体。

系统组成如图 1，包括：(1) 密码服务代理，实现对终端用户的身份认证、加解密操作、产生双方的会话密钥；(2) 应用服务器(AS)，存储系统的信息资源；(3) 密钥管理中心(KMC)，负责系统中的密钥管理，配置与系统中每一数字移动终端用户共享的端端密钥 $K_{C,\mathrm{KMC}}$，以及与应用服务器共享的端端密钥 $K_{\mathrm{AS,KMC}}$；(4) 数字移动终端用户(C)。依托密钥管理中心，通过密码服务代理完成移动终端身份认证，建立会话密钥，继而实现秘密数据的传输。

图 1 系统组成

2 协议的设计

鉴于数字移动通信中应用服务器对用户身份进行认证的特点，通过深入的分析研究，设计了一个身份认证协议，该协议与现有协议相比一个显著的特点是首先基于公钥密码体制设计了一个端端密钥分发协议。然后在此基础上基于对称密码体制设计了一个身份认证协议。这样设计的优点在于既完成了移动用户和应用服务器之间的双向认证，又通过利用一次性公钥证书保证了消息的新鲜性；同时移动用户加

2005-03-28 收到，2006-04-10 改回

密采用的是 RSA 公开密钥体制，解密采用的是单密钥体制，使得移动用户的计算量比较小，而且协议的安全性没有降低。

文中 N_U 表示主体 U 产生的一个随机数，$\{X\}_K$ 为对称密钥 K 对 X 加密的结果，$K_{A,B}$ 表示用户 A 和 B 共享的密钥。$(e_{A1},n_{A1}),(d_{A1},n_{A1})$ 为用户 A 在 RSA 公钥算法中的签名密钥对，$(e_{A2},n_{A2}),(d_{A2},n_{A2})$ 为用户 A 在 RSA 公钥算法中的通信密钥对；$(e_{B1},n_{B1}),(d_{B1},n_{B1})$ 为用户 B 在 RSA 公钥算法中的签名密钥对，$(e_{B2},n_{B2}),(d_{B2},n_{B2})$ 为用户 B 在 RSA 公钥算法中的通信密钥对；T_A,T_B 为时间标识。

设计的端端密钥分发协议如下：用户 A 和 B 相互验证从 CA 中心获得的证书的合法性，然后启动会话密钥产生分配子程序。图 2 中所使用的 RSA 算法和 Diffie-Hellman 算法以及各种符号都与文献[6]方案中完全相同。

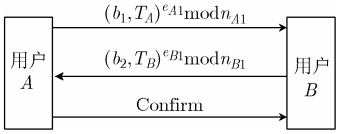

图 2 端端密钥分发协议

(1)用户 A 产生随机数 Rand$A$，利用 Diffie-Hellman 算法可得 $b_1=a^{\mathrm{Rand}A}\bmod P$，然后发送 $(b_1,T_A)^{e_{A1}}\bmod n_{A1}$ 给用户 B。

用户 B 产生随机数 Rand$B$，利用 Diffie-Hellman 算法可得 $b_2=a^{\mathrm{Rand}B}\bmod P$，然后发送 $(b_2,T_B)^{e_{B1}}\bmod n_{B1}$ 给用户 A。

(2)用户 A 将收到的 $(b_2,T_B)^{e_{B1}}\bmod n_{B1}$ 利用 (d_{B1},n_{B1}) 解密，对得到的时间标识 T_B 进行验证，并计算 $K_A=b_2^{\mathrm{Rand}A}\bmod P$。

用户 B 将收到的 $(b_1,T_A)^{e_{A1}}\bmod n_{A1}$ 利用 (d_{A1},n_{A1}) 解密，对得到的时间标识 T_A 进行验证，并计算 $K_B=b_1^{\mathrm{Rand}B}\bmod P$。

(3)完成上述步骤后，A 向 B 发出确认消息 Confirm，确认安全信息交换成功。双方以 $K_A=K_B$ 作为共享的端端密钥 $K_{A,B}$。其中消息 Confirm 是 A 在对 B 的身份真实性进行验证之后，向 B 发送的认证消息。

利用上述协议，可以在密钥管理中心(KMC)与每个数字移动终端用户(C)，以及应用服务器(AS)之间完成端端密钥 $K_{C,\mathrm{KMC}}$ 和 $K_{\mathrm{AS,KMC}}$ 的分发。

当网络系统中任何数字移动终端用户 C，密钥管理中心(KMC)和应用服务器(AS)之间利用上述协议，都分别完成了 $K_{C,\mathrm{KMC}}$ 和 $K_{\mathrm{AS,KMC}}$ 配置后，设计相应的身份认证协议如下：

$M1$ $C\rightarrow$AS：C, N_C

$M2$ AS→KMC：C, AS, N_C, N_{AS}

$M3$ KMC→AS：AS, N_{AS}，$\{C,\mathrm{AS},N_c,K_{c,\mathrm{AS}}\}_{K_{C,\mathrm{KMC}}}$，$\{C,\mathrm{AS},N_C,K_{C,\mathrm{AS}}\}_{K_{C,\mathrm{KMC}}}$

$M4$ AS→C：N_C，$\{C,\mathrm{AS},N_C,K_{C,\mathrm{AS}}\}_{K_{C,\mathrm{KMC}}}$，$\{N'_{\mathrm{AS}}\}_{K_{C,\mathrm{AS}}}$

$M5$ $C\rightarrow$AS：$\{N'_{\mathrm{AS}}-1\}_{K_{C,\mathrm{AS}}}$

第 1 步 C 产生一个随机数 N_C，连同身份标识符 C 与 N_C 一起明传给 AS。

第 2 步 AS 收到 C 与 N_C 后，产生一个随机数 N_{AS}，并将 C, AS, N_C, N_{AS} 一起明传给 KMC。

第 3 步 KMC 收到 C, AS, N_C, N_{AS} 后，产生一个用于 C 与 AS 之间一次通信的会话密钥 $K_{C,\mathrm{AS}}$，将 C, AS, N_{AS}, $K_{C,\mathrm{AS}}$ 和 C, AS, N_C, $K_{C,\mathrm{AS}}$ 分别用密钥 $K_{\mathrm{AS,KMC}}$ 和 $K_{C,\mathrm{KMC}}$ 加密，并将加密结果连同 AS 与 N_{AS} 一起传送给 AS。这里 N_{AS} 的作用有两个：一是向 AS 保证消息中报文$\{C,\mathrm{AS},N_{\mathrm{AS}},K_{C,\mathrm{AS}}\}_{K_{\mathrm{AS,\ KMC}}}$ 的新鲜性，二是让 AS 确认消息 $M3$ 确实来自 KMC，因为除 AS 外，只有 KMC 掌握密钥 $K_{\mathrm{AS,KMC}}$，因而也只有 KMC 能够将 N_{AS} 连同 C, AS, $K_{C,\mathrm{AS}}$ 正确加密。随机数 N_C 的作用与 N_{AS} 的作用类似，不再说明。

第 4 步 AS 收到报文$\{C,\mathrm{AS},N_{\mathrm{AS}},K_{C,\mathrm{AS}}\}_{K_{\mathrm{AS,\ KMC}}}$ 后，解密得到会话密钥 $K_{C,\mathrm{AS}}$，然后产生一个新的随机数 N'_{AS}，用会话密钥 $K_{C,\mathrm{AS}}$ 加密，将加密结果$\{N'_{\mathrm{AS}}\}_{K_{C,\mathrm{AS}}}$ 作为一个挑战连同从 KMC 处收到的报文$\{C,\mathrm{AS},N_C,K_{C,\mathrm{AS}}\}_{K_{C,\ \mathrm{KMC}}}$ 一起发给 C。

第 5 步 C 收到报文$\{C,\mathrm{AS},N_C,K_{C,\mathrm{AS}}\}_{K_{C,\ \mathrm{KMC}}}$ 后，解密得到会话密钥 $K_{C,\mathrm{AS}}$，再用 $K_{C,\mathrm{AS}}$ 将挑战$\{N'_{\mathrm{AS}}\}_{K_{C,\mathrm{AS}}}$ 解密，并传送响应$\{N'_{\mathrm{AS}}-1\}_{K_{C,\mathrm{AS}}}$ 给 AS。

其中应用服务器端的所有相关密码操作都是由密码服务代理完成的。在协议的第 4 步，C 收到$\{C,\mathrm{AS},N_C,K_{C,\mathrm{AS}}\}_{K_{C,\mathrm{KMC}}}$ 后，将其解密得到 AS 和 N_C，说明该消息的确来自 AS，即 C 完成了对 AS 的身份认证；在协议的第 5 步，AS 收到$\{N'_{\mathrm{AS}}-1\}_{K_{C,\mathrm{AS}}}$ 后对其解密得到 $N'_{\mathrm{AS}}-1$，从而完成了对用户 C 的认证。

总之，该协议通过密钥管理中心完成数字移动终端用户 C 和应用服务器 AS 之间的身份认证，同时建立双方通信用的会话密钥。下面对该认证协议的安全性进行详细的分析和证明。

3 认证协议的 Spi 演算分析

3.1 Spi 演算语法与证明规则

Spi 演算[7]是用密码学概念对 Pi 演算[8]进行扩展，Pi 演算引入了通道和范围的概念，是并发计算的基础。密码运算和通道通信是 Spi 演算的主要部分，其通道原语描述简单但功能强大。Spi 演算方法具有更为直观和精确的语义，使得密码协议的验证更加简单，而且 Spi 演算的协议模型是简洁和精练的。

由于协议的描述模型是繁琐的且可能导致新的二义性和错误，因此 Spi 演算的一个显著特点是不必给出协议的环境模型。特别地，对于环境中可以引入的任意数量的不能猜测协议秘密的成员的描述是困难的，对此 Spi 演算给出了如下的解决方法：假设环境为一个任意的 Spi 演算进程。Spi

演算的独特之处在于：依靠功能强大的 Pi 演算的范围概念，将环境定义为一个任意的 Spi 演算进程，以及 Spi 演算在增加描述基于共享密钥密码协议原语的基础上，使用等价关系来表示协议的认证性和秘密性，并利用测试等价方法，简化了密码协议的验证。Spi 演算是建立在标准并发形式之上的，与其他推理证明方法相比显然是优越的。

Spi演算的语法主要有两类，一类是项，用L, M, N表示；另一类是进程，用P, Q, R表示；m, n, q表示名字集合，x, y, z表示变量集合，$\{M\}_N$ 表示加密项，case L of$\{x\}_N$ in P表示解密进程。Spi演算的形式化语义主要有反应关系→，测试等价关系≃，barb等价关系≈，barb一致性~，结构等价关系≡和支持关系 —。

对于 Spi 演算的语法和形式化语义的定义及推理规则、定理，文献[7,9]中有详细的介绍，这里不再逐一介绍。

在分析协议的安全性时，给出下述两个定理。

定理 1　(1)barb 等价关系是自反的、传递的、对称的。(2)结构等价关系包含 barb 等价关系。(3)强互似性包含 barb 等价关系。(4)barb 等价关系受限定保护[1]。

定理 2　(1)barb 一致性是自反的、传递的、对称的。(2)barb 一致性是关于闭进程的一致性。(3)结构等价关系包含 barb 一致性。(4)强互似性包含 barb 一致性。(5)barb 一致性包含测试等价关系。

利用 Spi 演算方法，对 Needham-Schroeder 认证协议，MSR 认证协议，Kerberos 协议，Beller-Yacobi 认证协议，Aziz-Diffie 认证协议等协议进行了分析和验证，证实了这些协议已知的漏洞，这说明 Spi 演算方法对密码协议验证的结果是正确的和有效的，而且其验证过程相当简单。

3.2 协议的 Spi 演算分析

为便于分析，将协议分为(AS，KMC)和(C，AS)两部分，同时将 $M1$ 和 $M2$ 省去(不影响协议的分析)。

(1) 协议的 Spi 演算描述

第 1 部分　$M3$　KMC→AS：$\mathrm{AS}, N_{\mathrm{AS}}, \{C, \mathrm{AS}, N_{\mathrm{AS}}, K_{C,\mathrm{AS}}\}_{K_{\mathrm{AS,KMC}}}, \{C, \mathrm{AS}, N_C, K_{C,\mathrm{AS}}\}_{K_{C,\mathrm{KMC}}}$

$$\mathrm{KMC}(M) \triangleq (v\ K_{\mathrm{AS,KMC}})\overline{C_{\mathrm{AS}}} < \mathrm{AS}, N_{\mathrm{AS}}, \{M\}_{K_{\mathrm{AS,KMC}}}, \{C, \mathrm{AS}, N_C, K_{C,\mathrm{AS}}\}_{K_{\mathrm{C,KMC}}} >$$

$$\mathrm{AS} \triangleq C_{\mathrm{AS}}(\mathrm{AS}, N_{AS}, y_{\mathrm{cipher}}, x_{\mathrm{cipher}})\mathrm{case}\, y_{\mathrm{cipher}}\, \mathrm{of}\ \{C, \mathrm{AS}, N_{\mathrm{AS}}, y\}_{K_{\mathrm{AS,KMC}}}\ \mathrm{in}\, F(y)$$

$$\mathrm{Sys}(M) \triangleq (v\ K_{C,\mathrm{AS}})(v\ K_{\mathrm{AS,KMC}})(\mathrm{KMC}(M)|\mathrm{AS})$$

$$\mathrm{AS}_{\mathrm{spec}}(M) \triangleq C_{\mathrm{AS}}(\mathrm{AS}, N_{\mathrm{AS}}, y_{\mathrm{cipher}}, x_{\mathrm{cipher}})\mathrm{case}\, y_{\mathrm{cipher}}\, \mathrm{of}\ \{C, \mathrm{AS}, N_{\mathrm{AS}}, y\}_{K_{\mathrm{AS,KMC}}}\ \mathrm{in}\, F(M)$$

$$\mathrm{Sys}_{\mathrm{spec}}(M) \triangleq (v\ K_{C,\mathrm{AS}})(v\ K_{\mathrm{AS,KMC}})(\mathrm{KMC}(M) \mid \mathrm{AS}_{\mathrm{spec}}(M))$$

第 2 部分　$M4$　$\mathrm{AS} \to C: N_C, \{C, \mathrm{AS}, N_C, K_{C,\mathrm{AS}}\}_{k_{C,\mathrm{KMC}}}, \{N'_{\mathrm{AS}}\}_{K_{C,\mathrm{AS}}}$

$M5$　C→AS：$\{N'_{\mathrm{AS}} - 1\}_{K_{C,\mathrm{AS}}}$

$$\mathrm{AS}(M) \triangleq (v\ K_{C,\mathrm{KMC}})\ \overline{C_C} < N_C, \{C, \mathrm{AS}, N_C, K_{C,\mathrm{AS}}\}_{K_{C,\mathrm{KMC}}}, \{M\}_{K_{C,\mathrm{AS}}} >$$

$$C \triangleq C_C(N_C, x_{\mathrm{cipher}}, z_{\mathrm{cipher}})\mathrm{case}\ x_{\mathrm{cipher}}\ of\{C, \mathrm{AS}, N_C, y\}_{K_{C,\mathrm{KMC}}}\ \mathrm{in\ case}\, z_{\mathrm{cipher}}\ \mathrm{of}\ \{N'_{\mathrm{AS}}\}_y \mathrm{in}\ \overline{C_C} < \{N'_{\mathrm{AS}} - 1\}_y > F(y)$$

$$\mathrm{Sys}(M) \triangleq (v\ K_{C,\mathrm{AS}})(v\ K_{C,\mathrm{KMC}})(AS(M) \mid C)$$

$$C_{\mathrm{spec}}(M) \triangleq C_C(N_C, x_{\mathrm{cipher}}, z_{\mathrm{cipher}})\mathrm{case} x_{\mathrm{cipher}}\ \mathrm{of}\ \{C, AS, N_C, y\}_{K_{C,\mathrm{KMC}}}\ \mathrm{in\ case}\, z_{\mathrm{cipher}}\ of\ \{N'_{\mathrm{AS}}\}_y \mathrm{in}\ \overline{C_C} < \{N'_{\mathrm{AS}} - 1\} > F(y)$$

$$\mathrm{Sys}_{\mathrm{spec}}(M) \triangleq (v\ K_{C,\mathrm{AS}})(v\ K_{C,\mathrm{KMC}})(\mathrm{AS}(M) \mid C_{\mathrm{spec}}(M))$$

(2) 协议的安全性定义　在分析协议的安全性时，考虑两个性质：即保密性和认证。保密性根据下述等价关系定义：如果 $F(M) \simeq F(M')$，则对所有的 M 和 M'，$\mathrm{Sys}(M) \simeq \mathrm{Sys}(M')$；认证由下述等价关系保证：对所有的 M, $\mathrm{Sys}(M) \simeq \mathrm{Sys}_{\mathrm{spec}}(M)$。

(3) 安全性证明　首先对协议第一部分的认证及保密性证明。

定理 3(认证)　对所有的闭项 M，$\mathrm{Sys}(M) \simeq \mathrm{Sys}_{\mathrm{spec}}(M)$

证明　令 $\delta = \{\mathrm{AS}, N_{\mathrm{AS}}, \{M\}_{K_{\mathrm{AS,\ KMC}}}/x, \{C, \mathrm{AS}, N_C, K_{C,\mathrm{AS}}\}_{K_{C,\mathrm{KMC}}}\}$，$R$ 是任一闭进程，且 $K_{\mathrm{AS,KMC}} \notin f_n(R)$，并引入下述关系 Σ：

$P \Sigma Q$　iff　$P = \mathrm{AS}|\, R_1\ \delta$ 和 $Q = \mathrm{AS}_{\mathrm{spec}}(M)|\, R_1\ \delta$，对某个 R_1 使得 $x\{\text{-}\}_{K_{\mathrm{AS,\ KMC}}} \vdash R_1$。首先给出 P 的反应关系：

(1) 如果 $R_1\ \delta\ \overline{C_{\mathrm{AS}}}\,(v\vec{n})\langle N\rangle R'$ 和 $P' \equiv (v\vec{n})(\mathrm{case}\ N\ \mathrm{of}\ \{C, \mathrm{AS}, N_{\mathrm{AS}}, y\}_{K_{\mathrm{AS,\ KMC}}}\ \mathrm{in}\ F(y)|\, R')$，则 $P \to P'$。

(2) 如果 $R_1\ \delta \not\to R'$ 和 $P' \equiv \mathrm{AS}|\, R'$，则 $P \to P'$。

对 P 的这两种情形，分别证明 Q 均能和 P 匹配。

(1) Q 的反应关系：$Q \to Q' \triangleq (v\vec{n})(\mathrm{case}\ N\ \mathrm{of}\ \{C, \mathrm{AS}, N_{\mathrm{AS}}, y\}_{K_{\mathrm{AS,\ KMC}}}\ \mathrm{in}\ F(M)|\, R')$

这里 N 分两种情况：密文和非密文。

(a)　N 为密文时，

$$\begin{aligned} P' &\equiv (v\vec{n})(\mathrm{case}\ \{M\}_{K_{\mathrm{AS,\ KMC}}}\ \mathrm{of}\ \{C, \mathrm{AS}, N_{\mathrm{AS}}, y\}_{K_{\mathrm{AS,\ KMC}}}\ \mathrm{in}\ F(y)|\, R') \\ &\equiv (v\vec{n})(F(M)|\, R') \\ &\equiv (v\vec{n})(\mathrm{case}\ \{M\}_{K_{\mathrm{AS,\ KMC}}}\ \mathrm{of}\ \{C, \mathrm{AS}, N_{\mathrm{AS}}, y\}_{K_{\mathrm{AS,\ KMC}}}\ \mathrm{in}\ F(M)|\, R') \\ &\equiv Q' \end{aligned}$$

(b) N 为非密文时，

$$P' \equiv (v\vec{n})(\mathrm{case}\ N\ \mathrm{of}\ \{C, \mathrm{AS}, N_{\mathrm{AS}}, y\}_{K_{\mathrm{AS,\ KMC}}}\ \mathrm{in}\ F(y)|\, R') \approx (v\vec{n})(0|\, R') \approx (v\vec{n})(\mathrm{case}\ N\ \mathrm{of}\ \{C, \mathrm{AS}, N_{\mathrm{AS}}, y\}_{K_{\mathrm{AS,\ KMC}}}\ \mathrm{in}\ F(M)|\, R') \equiv Q'$$

由定理 1 可得 $P' \approx Q'$

(2) Q 的反应关系：$Q \to Q' \triangleq \mathrm{AS}_{\mathrm{spec}}(M)|\, R'$

存在 R'_1 使得 $x\{\text{-}\}_{K_{\mathrm{AS,\ KMC}}} \vdash R'_1$ 且 $R'_1\ \delta = R'$，因此 $(\mathrm{AS}|\ R')\ \Sigma\ Q'$，所以 $P' \equiv \Sigma \equiv Q'$。

同理，也可证明 P 能匹配 Q 的反应关系。

至此$\Sigma \bigcup \dot{\approx}$是一个 barb 互模拟，由定理 1 可得$\Sigma \subseteq \dot{\approx}$。

其次令 $R_1 = \overline{C_{\mathrm{AS}}} <x> \mid R$，可得

$(\overline{C_{\mathrm{AS}}} <\mathrm{AS}, N_{\mathrm{AS}}, \{M\}_{K_{\mathrm{AS,KMC}}}, \{C, \mathrm{AS}, N_C, K_{C,\mathrm{AS}}\}_{K_{C,\mathrm{KMC}}} > |\mathrm{AS}|R) \equiv (\mathrm{AS}|\, R_1\ \delta)$

$\Sigma(\mathrm{AS}_{\mathrm{spec}}(M)|\, R_1\ \delta) \equiv (\overline{C_{\mathrm{AS}}} <\mathrm{AS}, N_{\mathrm{AS}}, \{M\}_{K_{\mathrm{AS,\ KMC}}}, \{C, \mathrm{AS}, N_C, K_{C,\mathrm{AS}}\}_{K_{C,\mathrm{KMC}}} > |\mathrm{AS}_{\mathrm{spec}}(M)|\ R)$

$(\overline{C_{\mathrm{AS}}} <\mathrm{AS}, N_{\mathrm{AS}}, \{M\}_{K_{\mathrm{AS,\ KMC}}}, \{C, \mathrm{AS}, N_C, K_{C,\mathrm{AS}}\}_{K_{C,\mathrm{KMC}}} > |\mathrm{AS}|\ R) \dot{\approx} (\overline{C_{\mathrm{AS}}} <\mathrm{AS}, N_{\mathrm{AS}}, \{M\}_{K_{\mathrm{AS,\ KMC}}}, \{C, \mathrm{AS}, N_C, K_{C,\mathrm{AS}}\}_{K_{C,\mathrm{KMC}}} > |\mathrm{AS}_{\mathrm{spec}}(M)|\ R)$

由定理 1(2)和$\Sigma \subseteq \dot{\approx}$，可得 $\mathrm{Sys}(M)|R \dot{\approx} \mathrm{Sys}_{\mathrm{spec}}(M)|R$ 和 $\mathrm{Sys}(M) \dot{\approx} \mathrm{Sys}_{\mathrm{spec}}(M)$，由 barb 一致性的定义和定理 2(5)得到

$$\mathrm{Sys}(M) \simeq \mathrm{Sys}_{\mathrm{spec}}(M) \tag{1}$$

为了证明保密性，先证明它的一个限定情形。

引理 1 如果对任意闭项 M, M'，$F(x)$是$\overline{c} <*>$，则 $\mathrm{Sys}(M) \simeq \mathrm{Sys}(M')$。

证明 证明过程与定理 3 的证明方法相同。

保密性的完整证明如下。

定理 4(保密性) 对任意闭项 M, M'，如果 $F(M) \triangleq F(M')$,

则 $\mathrm{Sys}(M) \simeq \mathrm{Sys}(M')$。

证明 假定 c 是一个新鲜名字，y 是一个新鲜变量

$$\begin{aligned}
\mathrm{Sys}_{\mathrm{spec}}(N) &= (\nu\ C_{\mathrm{AS}})(\overline{C_{\mathrm{AS}}} <N>.0|\, C_{\mathrm{AS}}(x).\ F(N)) \\
&\simeq (\nu\ C_{\mathrm{AS}})(\overline{C_{\mathrm{AS}}} <N>.0|\, C_{\mathrm{AS}}(x).\ (\tau.F(N))) \\
&\simeq (\nu\ C_{\mathrm{AS}})(\overline{C_{\mathrm{AS}}} <N>.0|\, (\nu\ c)(C_{\mathrm{AS}}(x).\ \overline{c} <*> \mid \\
&\quad c(y).\ F(N))) \\
&\equiv (\nu\ c)\ (\nu\ C_{\mathrm{AS}})((\overline{C_{\mathrm{AS}}} <N>.0|\, C_{\mathrm{AS}}(x).\ \overline{c} <*>) \mid \\
&\quad c(y).\ F(N)) \\
&= (\nu\ c)(\mathrm{Sys}(N,(x)\ \overline{c} <*>)|\ c(y).\ F(N))
\end{aligned}$$

由引理 1、定理 3 及 $F(M) \simeq F(M')$，可得

$$\begin{aligned}
\mathrm{Sys}(M) &\simeq \mathrm{Sys}_{\mathrm{spec}}(M) \\
&\simeq (\nu\ c)\ (\mathrm{Sys}\ (M, (x)\ \overline{c} <*>)|\ c(y).\ F(M)) \\
&\simeq (\nu\ c)\ (\mathrm{Sys}\ (M', (x)\ \overline{c} <*>)|\ c(y).\ F(M') \\
&\simeq \mathrm{Sys}_{\mathrm{spec}}(M') \simeq \mathrm{Sys}(M')
\end{aligned} \tag{2}$$

由式(1)和式(2)，证明了协议的第 1 部分(AS, KMC)是安全的。同理可以证明协议的第 2 部分(C, AS)也是安全的。

通过以上证明，整个协议达到了预期的目标。

4 结束语

本文针对数字移动通信系统的背景和需求，基于非对称密码体制，设计了一个端端密钥分发协议；基于对称密码体制，设计了一个查询系统的认证协议。认证协议依托系统的密钥管理中心，完成查询用户与应用服务器间的身份认证，同时建立会话密钥，并利用 Spi 演算对所设计的认证协议进行了分析，结果表明该协议是安全的。

参 考 文 献

[1] Boyd C and Mathuria A. Protocols for Authentication and Key Establishment. Springer, 2003: 33–72.

[2] Basyouni A. Analysis of wireless cryptographic protocols. [Master thesis], Kingson, Ontario, Queen's University, Canada, 1997.

[3] Mu Y and Varadharajan V. On the design of security for mobile communications. ACISP'96, Australia, 1996: 134–145.

[4] Brown D. Techniques for privacy and authentication in personal communication systems. *IEEE Personal Communications*, 1995, 2(4): 6–10.

[5] Mao WenBo. Modern Cryptography: Theory and Practice(英文版). 北京: 电子工业出版社. Beijing: Publishing House of Electronics Industry, 2004: 367–382.

[6] Burrows M, Abadi M, and Needham R. A logic of authentication. Proceedings of the Royal Society of London A, 1989, 426(1871): 233–271.

[7] Abadi M and Gordon A. A calculus for cryptographic protocols: The Spi calculus. *Journal of Information and Computation*, 1999, 148(1): 1–70.

[8] Milner R, Parrow J, and Walker D. A calculus for mobile processes, part I/II. *Journal of Information and Communication*, 1992, 100(1): 1–77.

[9] Blanchet B. From secrecy to authenticity in security protocols. Proceedings of SAS'02, 2002, LNCS 2477: 342–359.

王全来： 男，1970 年生，博士生，研究方向为密码学、信息安全.

韩继红： 女，1966 年生，副教授，主要研究方向为信息系统安全.

王亚弟： 男，1953 年生，教授，博士生导师，研究方向为密码学、信息安全.