doi: 10.7690/bgzdh.2016.11.013

一种用户身份保密加强的 LTE 认证与密钥协商方案

朱诗兵[1]，周　赤[2]，李长青[1]
（1. 装备学院信息装备系，北京 101416；2. 陆军航空兵学院指挥系，北京 101100）

摘要：为了保护用户身份隐私，提出一种用户身份保密加强的 LTE 认证与密钥协商方案。通过分析 EPS AKA 的具体流程以及 LTE 认证与密钥协商（AKA）协议机制，发现其存在安全缺陷，提出了用户身份保密 AKA（UICE-AKA）方案。方案中在 HSS 增加 RMM，用以产生 RIC，以生成动态移动用户身份识别码（DMSI），设计一种 LTE 用户身份保密加强方案并进行安全性分析。分析结果表明：该方案有效保护了 IMSI，减小了其被攻击者截获的危险性，能够进一步保护 LTE 中的用户身份。

关键词：LTE；AKA；用户身份保密；DMSI
中图分类号：TP393.08　　**文献标志码：**A

LTE Authentication and Key Agreement Scheme with Enhanced User Identity Privacy

Zhu Shibing[1], Zhou Chi[2], Li Changqing[1]
(1. *Department of Information Equipment*, *Academy of Equipment*, *Beijing* 101416, *China*;
2. *Department of Command*, *Army Aviation School*, *Beijing* 101100, *China*)

Abstract: In order to protect the user privacy, a LTE user identity enhanced authentication and key agreement scheme is proposed. By analyzing the specific process of EPS AKA and the mechanism of LTE AKA protocol, it is found that there are security flaws, and the user identity secret AKA (UICE-AKA) scheme is proposed. In the scheme, the HSS is added to RMM, which is used to generate RIC, to generate dynamic mobile user identity identification code (DMSI), and to design a LTE user identity privacy enhancing scheme and security analysis. Analysis results show that the proposed scheme can effectively protect the IMSI, reduce the risk of the attacker's interception, and can further protect the user identity in LTE.

Keywords: LTE; AKA; user identity confidentiality; DMSI

0　引言

在全球移动通信系统（global system for mobile communication，GSM）和通用移动通信系统（universal mobile telecommunication system，UMTS）中，有些情况下，用户的永久身份是以明文形式在空口传送的[1]。永久身份的明文传送是一个安全缺口，并对用户身份隐私造成威胁。笔者将分析长期演进系统（long term evolution，LTE）的认证与密钥协商协议（EPS AKA[1]），可以看到对用户身份保密的威胁在 LTE 中同样存在；因此，笔者提出一种用户身份保密的加强方案，以进一步保护 LTE 中的用户身份。

1　EPS AKA 过程

EPS AKA 源于 3GPP AKA，延用了常用的“挑战/响应”机制[2]。通过网络与用户设备之间的协商认证，得到密钥，为后续的通信加密做好准备工作，保障通信的安全。

如图 1 所示，EPS AKA 具体流程[3]如下：

1) 用户设备（user equipment，UE）向移动性管理实体（mobility management entity，MME）发送接入请求，传递 IMSI 与 ID_{HSS} 标识等身份信息；

2) MME 通过认证数据请求将 IMSI，SN id（服务网标志）和 Network Type（服务网类型）传送给 HSS（归属用户服务器）；

3) HSS 收到认证数据请求后，检查 IMSI 与 SN id 是否合法。检查通过，则生成认证向量组 AV(1, …, n)，并作为对认证数据的应答返回给 MME。

认证向量包括参数 AUTN（authentication token，认证令牌）、RAND（随机数）、密钥 K_{ASME}（用来产生非接入层和接入层密钥的基础密钥）和 XRES（通过和用户返回的 RES 比较来达成密钥协商的目的）。生成认证向量组 AV(1,…,n)的相关参数算法[4]如下：

$$MAC = f1_k(SQN \| RAND \| AMF)；\quad (1)$$

$$XRES = f2_k(RAND)；\quad (2)$$

$$K_{ASME} = KDF(f3_k(RAND), f4_k(RAND))；\quad (3)$$

收稿日期：2016-07-01；修回日期：2016-08-05
作者简介：朱诗兵（1969—），男，湖南人，博士，教授，从事信息与通信系统研究。

$$AK = f5_k(RAND)。 \quad (4)$$

获得参数后，根据以下方法计算 AUTN 与 AV：

$$AUTN = SQN \oplus AK \| AMF \| MAC； \quad (5)$$

$$AV = RAND \| XRES \| K_{ASME} \| AUTN。 \quad (6)$$

4) MME 收到 HSS 送来的向量 AV 后，按序选择一组 AV 向量 AV(i)，提取出 $K_{ASME}(i)$、RAND(i)、AUTN(i)等数据，同时为 $K_{ASME}(i)$分配一个密钥标志 $KSI_{ASME}(i)$，然后向用户设备发送认证请求。

5) 用户设备收到认证请求后，通过提取 AUTN(i)中的 MAC 等信息，并计算 XMAC，比较 XMAC 和 MAC 是否相等，同时验证序列号 SQN 取值是否正常。如果认证通过，则计算 RES(i)与 $K_{ASME}(i)$，并将 RES(i)传输给 MME。

$$XMAC = f1_k(SQN \| RAND \| AMF)； \quad (7)$$

$$RES = f2_k(RAND)。 \quad (8)$$

6) MME 将收到的 RES(i)与 AV(i)中的 XRES(i)进行比较，如果一致，则通过认证；接下来 MME 和用户设备演算得到 $K_{ASME}(i)$，并以 $K_{ASME}(i)$作为基础密钥，推算出完整性保护密钥和加密密钥，然后开启安全模式命令(SMC)。

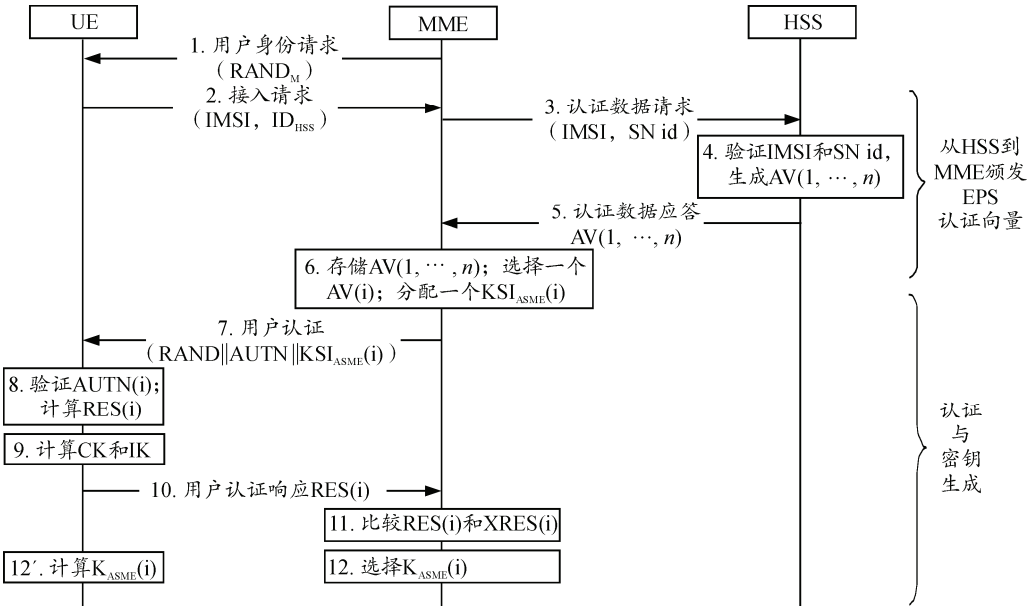


图 1 EPS AKA 流程

2 EPS AKA 的安全缺陷

虽然 EPS AKA 相对 3G 做了很多改进，但仔细分析，其仍然存在一些安全缺陷：

1) IMSI 在无线信道中以明文形式传输，易被攻击者截获；2) 协议初始时，MME 未及时对 UE 进行认证，易引发拒绝服务攻击；3) UE 与 HSS 的公共密钥 K 长期共存，易被破获；4) MME 和 HSS 之间传递的消息未经保护[5]。

在以上漏洞中，威胁最大的是 IMSI 泄露，这是因为一旦 IMSI 被不法攻击者截获，攻击者就可以利用截获的 IMSI 伪装成合法用户访问网络，而其他 3 个方面的加强都无法阻止这种攻击。IMSI 之于整个 AKA 过程来说就像是一把钥匙，其他方面就像是门，一旦钥匙掌握在攻击者手中，门再坚固都无法阻止攻击者入侵；因此，对 EPS AKA 的改进的第一要务就是对用户身份提供必要保护。为保证用户身份保密，需要对 UE 的 IMSI 进行保护，不能以明文形式传递。

3 用户身份保密加强 AKA 方案设计

3.1 动态移动用户识别码 DMSI

EPS AKA 身份保护机制如图 2 所示，MME 与 HSS 需要传输 IMSI[6]。在本方案中，动态移动用户识别码(dynamic mobile subscriber identity，DMSI)将代替 IMSI 传输。如图 3 所示，笔者向当前的 EPS AKA 密钥体系中添加了中间用户身份(即 DMSI)。当需要传输 IMSI 时，现都改为传输 DMSI。这样一来，明文的 IMSI 就不会暴露在任何接口处，MME 也无法获知 IMSI。

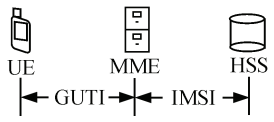


图 2 EPS AKA 身份保护机制

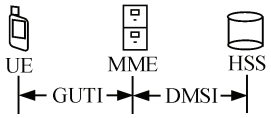


图 3　用户保密加强改进方案

EPS AKA 过程中，随着 UE 收到的最新的随机数的改变，DMSI 的值一直在改变[7]。由于 DMSI 的值一直在变化，获知前一个 DMSI 将不会对用户的永久身份造成威胁。定义 DMSI 组成部分中的变化因子为身份保密随机码(Random number for Identity Confidentiality，RIC)。DMSI 的构成如下：

$$\mathrm{DMSI}=\mathrm{MCC}\|\mathrm{MNC}\|\mathrm{RIC}\text{。} \tag{9}$$

其中：跟 IMSI 中一样，MCC 表示移动国家代码；MNC 表示移动网络代码；而 RIC 表示身份保密随机码。

身份保密随机码(random number for identity confidentiality，RIC)是一个随机数，在一段时间内能唯一确定在某一特定 HE(Home Environment，本地环境)中的 UE 的身份[8]。

每生成一个新的认证向量，就会有一个新的 RIC 产生，而 RIC-IMSI 之间的联系将存储在 HSS 的数据库之中。认证向量包括 RAND、AUTN、XRES、K_{ASME} 等 4 个参数。RIC 主要由存在于 HSS 中的 RIC 管理模块 RMM(RIC manager module)产生，HSS 收到 UE 的 RIC 后，根据 RIC-IMSI 的关系，获得用户的信息，并且由 RMM 生成新的 RIC。

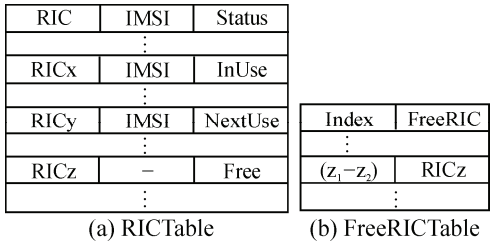
3.2　RIC 管理模块——RMM 及其工作原理

RIC 管理模块(RMM)是用来处理与 RIC 相关的函数的，存在于 HE 中[9]。它为每个 UE 存储并管理着 2 个 RIC：当前 RIC(InUse)和下一轮 RIC(NextUse)。他们都跟 UE 的 IMSI 存在着对应关系。RMM 中有 2 个表格，具体如下：

1) RIC 表格。

第 1 个表格为 RICTable (RIC, IMSI, Status, PairRIC)，它包含了系统中所有可用的 RIC，如图 4(a)所示。RIC 用来作为表格索引，IMSI 表示用户的 IMSI，Status 表示相应 RIC 的状态，共有 3 种状态，分别为 InUse，NextUse 和 Free。每一行有一个状态为 InUse 和一个状态为 NextUse 的 RIC，剩下的所有 RIC 都处于 Free 状态，表示它们还没有被分配给任何一个 UE。

第 2 个表格包含第 1 个表格中所有 Free 状态的 RIC，表示为 FreeRICTable(Index, FreeRIC)，如图 4(b)。此表格用于在 NextRIC 请求过程中分配 RIC。



(a) RICTable　(b) FreeRICTable

图 4　RICTable 和 FreeRICTable 构成

2) 对请求的回应。

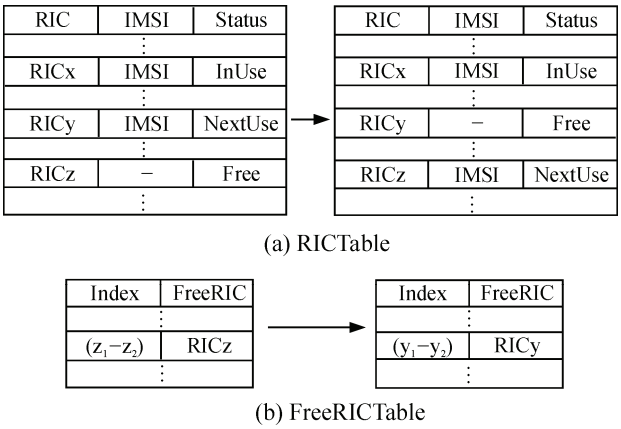
一旦 RMM 收到一个含有参数 RIC 的 IMSI 请求，由于 RIC 是 RICTable 的索引 RMM 可以很容易地从 RICTable 中找到相应的 IMSI。当 RMM 收到带有 RIC 的下一轮 RIC 请求时，它会启动 GetNextRIC 函数。GetNextRIC()的实现流程为：

① 在 RICTable 中查找到 RIC 的状态。

②如果其状态是 NextUse(即 RIC=RICy)，此函数将会产生一个随机数 RAND，并将这个数作为索引，以从 FreeRICTable 中获取一个新的 RIC(RICz)，并且将 RICx 释放到 FreeRICTable 中。

③ 更新 RICTable：将 RICy 行的状态变换为 InUse，并将 RICz 行的状态变换为 NextUse。由于 RICx 已经被释放到 FreeRICTable 中了，其状态会被变换为 Free。RMM 最终返回 RICz。

④ 如果 RIC 的状态为 InUse(即 RIC=RICx)，这是一个重复请求。在这种情况下，将重新进行 RICy 的计算。此情形通常在先前分配的 RIC 没有被 UE 成功接收的时候发生。



(a) RICTable

(b) FreeRICTable

图 5　RIC 为 InUse 时的表更新

注意：RIC 的状态为 NextUse 和 InUse 时，流程图中的“更新表”的具体实现步骤是不同的。

当 RIC 的状态为 InUse 时：

(RICy, IMSI, NextUse) → (RICy, –, Free)；

(RICz, –, Free) → (RICz, IMSI, NextUse)。

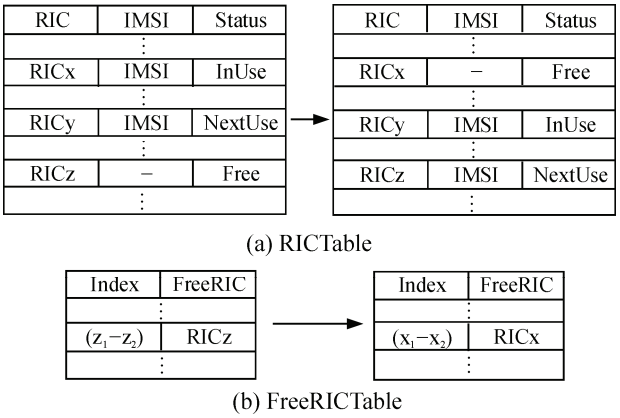


图 6　RIC 为 NextUse 时的表更新

如图 5 所示，当 RIC 的状态为 NextUse 时(即 RIC 为 RICy 时)：

(RICx, IMSI, InUse) → (RICx, –, Free)；

(RICy, IMSI, NextUse) → (RICy, IMSI, InUse)；

(RICz, –, Free) → (RICz, IMSI, NextUse)。

如图 6 所示。

5) 当 RIC 的状态为 Free 时，则出现错误，返回“ERROR”消息。

3.3　UICE-AKA 方案

当首次接入，TMSI 不能鉴定 UE 或 TMSI 跟与其相关联的 UE 之间的关联消失时，MME 会发起 UICE-AKA 过程[11]。下面，笔者将介绍 UICE-AKA 的实现步骤。

假设 UE 绑定的 2 个 RIC 分别为 RIC_x(处于 InUse 状态)和 RIC_y(处于 NextUse 状态)。有了这些假设，UICE-AKA 的实现步骤如图 7 所示。

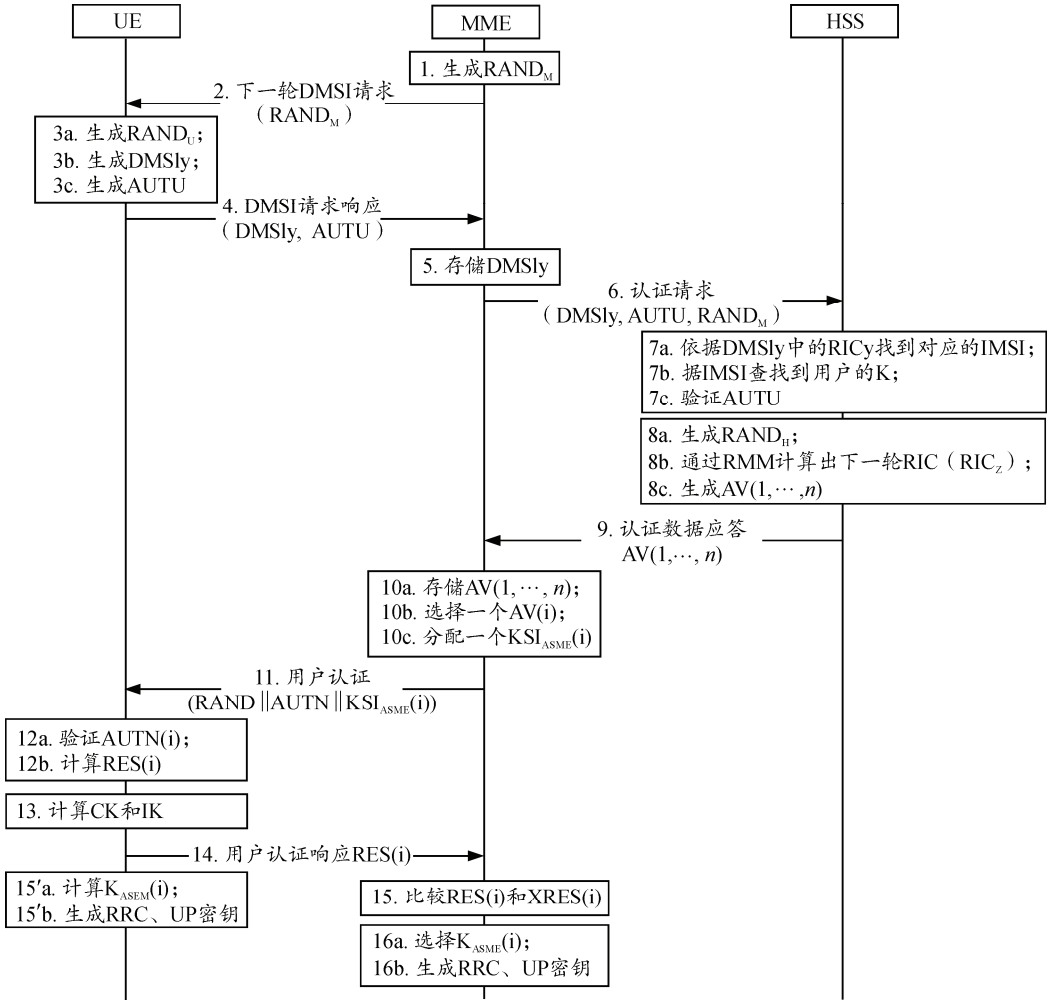


图 7　UICE-AKA 实现流程

图 7 中，步骤 1～3，MME 生成一个随机数 $RAND_M$。通过下一轮 DMSI 请求消息将其发送给 UE。接到请求后，UE 生成一个随机数 $RAND_U$，并计算：

$$MAC_{RIC_y} = f1_k(RIC_y \| RAND_U \| RAND_M)；\quad (10)$$

$$AUTU = RAND_U \| MAC_{RIC_y}。\quad (11)$$

图 7 中，步骤 4～7，随后 UE 向 MME 发送回

复消息，消息中包含 $DMSI_y$ 和用来认证 UE 的认证向量 AUTM。收到消息后，MME 临时存储 $DMSI_y$。MME 将收到的消息连同 $RAND_M$ 一同发送给 HSS。HSS 分离出 DMSIy 中的 RICy，并向 RMM 发送带有参数 RICy 的 IMSI 请求。得到对应的 IMSI，HSS 利用 IMSI 得到相应的 UE 的秘密密钥 K，并计算

$$XMAC_{RIC_y} = f1_k(RIC_y \| RAND_H \| RAND_M)。\quad (12)$$

比较 $XMAC_{RICy}$ 和 MAC_{RICy}，若相等，则 HSS 认证 UE 成功；因为只有真正的 UE 拥有 K，并利用其产生 MAC_{RICy}。

图 7 中，步骤 8～10，HSS 生成 $RAND_H$，并通过 RMM 计算出下一轮 RIC(RIC_z)，最后生成 AV(1,…,*n*)。HSS 向 MME 发送认证应答消息，包含 AV(1,…,*n*)。MME 收到 HSS 送来的向量 AV 后，按序选择一组 AV 向量 AV(i)，提取出 KASME(i)、RANDH(i)、AUTN(i)等数据，同时为 KASME(i)分配一个密钥标志 KSIASME(i)，然后向用户设备发送认证请求。

图 7 中，步骤 11～14，用户设备收到认证请求后，通过提取 AUTN(i)中的 MAC_{RICz} 等信息，计算 $XMAC_{RICz}$，比较 $XMAC_{RICz}$ 和 MAC_{RICz} 取值是否相等，同时验证序列号 SQN 取值是否正常。如果认证通过，则计算 RES(i)与 K_{ASME}(i)，并将 RES(i)传输给 MME。

其中：

$$XMAC_{RIC_z} = f1_k(SQN \| RAND_H \| AMF)；\quad (13)$$

$$RES = f2_k(RAND)。\quad (14)$$

图 7 中，步骤 15，MME 将收到的 RES(i)与 AV(i)中的 XRES(i)进行比较，如果一致，则通过认证。

4　UICE-AKA 安全性分析

1) 身份保密性。

① IMSI 机密性得以保护。在本方案中，DMSI 扮演了 IMSI 的角色，这样 IMSI 就不会在通信链路(无线或有线)中传输。另外，RMM 保证了在 DMSI 和 IMSI 之间不会有逻辑关系。任何其他人包括 MME 都无法获得 IMSI，维护了 IMSI 的机密性。

② DMSI 是不可追踪的。标签生存期有限；RIC 不会以明文形式在无线链路上传输；同一个 UE 的不同 RIC 之间没有逻辑关系；对于下一轮标签请求，RMM 返回 free 的 RIC 作为响应。这样就能避免不同标签之间产生联系。

2) 完整性保护。

在 UICE-AKA 中，传送消息的完整性通过 MAC 得以验证。MAC_{RICx} 和 MAC_{RICy} 同时保证了 RIC 和随机数的完整性；而且，在步骤 8 中，UE 可以通过 MAC_{RICy} 检验新标签 RIC_y 的完整性[11]。

3) 双向认证。

UICE-AKA 的第 7 步中，HSS 计算 $XMAC_{RICy}$ 并将其与包含在 AUTU 中的 MAC_{RICy} 比较。由于只有真正的 UE 才会知道 K 值并利用其计算 MAC_{RICy}，所以 HSS 可以因此认证 UE。相似的，在步骤 12 中，UE 验证包含在 AUTN 中的 MAC_{RICz} 的合法性，以此对网络进行认证(HSS 和 MME)。在步骤 15 中，MME 将 UE 生成的 RES 与 MME 收到的 XRES 进行比较，以认证用户。事实上，UICE-AKA 过程中实体之间建立起了双向认证。

5　结束语

笔者对所提方案(UICE-AKA)进行安全性分析。结果表明：该方案有效保护了 IMSI，减小了其被攻击者截获的危险性，能够进一步保护 LTE 中的用户身份。

参考文献：

[1] Forsberg D, Horn G, Moeller W D, et al. LTE security[M]. John Wiley & Sons, 2012: 101-105.

[2] 汪良辰. LTE 安全接入机制研究[D]. 西安: 西安电子科技大学, 2012: 56-60.

[3] Dai W. Crypto++ 5.6. 0 benchmarks[J]. Website at http://www. cryptopp. com/benchmarks. html, 2009 21(3): 1-4.

[4] 3GPP TS 33. 220 V10.1.0 (2012-03) Generic Authentication Architecture (GAA)[Z]. Generic Bootstrapping Architecture (GBA) (Release 10), 2012.

[5] 刘保菊，刘家磊. 基于口令的三方密钥交换协议的分析与研究[J]. 兵工自动化, 2014, 33(3): 36-39.

[6] 何青春，马治国. HMAC-SHA-256 算法在 TD-LTE 系统中的应用[J]. 现代电信科技, 2012 42(4): 32-35.

[7] 陈瑶瑶，郝建华，张子博，等. 端到端语音加密通信技术[J]. 四川兵工学报, 2015, 36(12): 103-108.

[8] 殷明勇，孔思淇，刘爱民，等. 基于故障树分析的网络系统可靠性研究[J]. 兵工自动化, 2014, 33(11): 44-45.

[9] Choudhury H, Roychoudhury B, Saikia D K. Enhancing user identity privacy in lte[C]//Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012: 949-957.

[10] Xiehua L, Yongjun W. Security enhanced authentication and key agreement protocol for LTE/SAE network[C]//Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on. IEEE, 2011: 1-4.

[11] 张记瑞，黄圣春，魏急波. 无线网格网 MAC 层协议研究[J]. 兵工自动化, 2015, 34(5): 29-32.