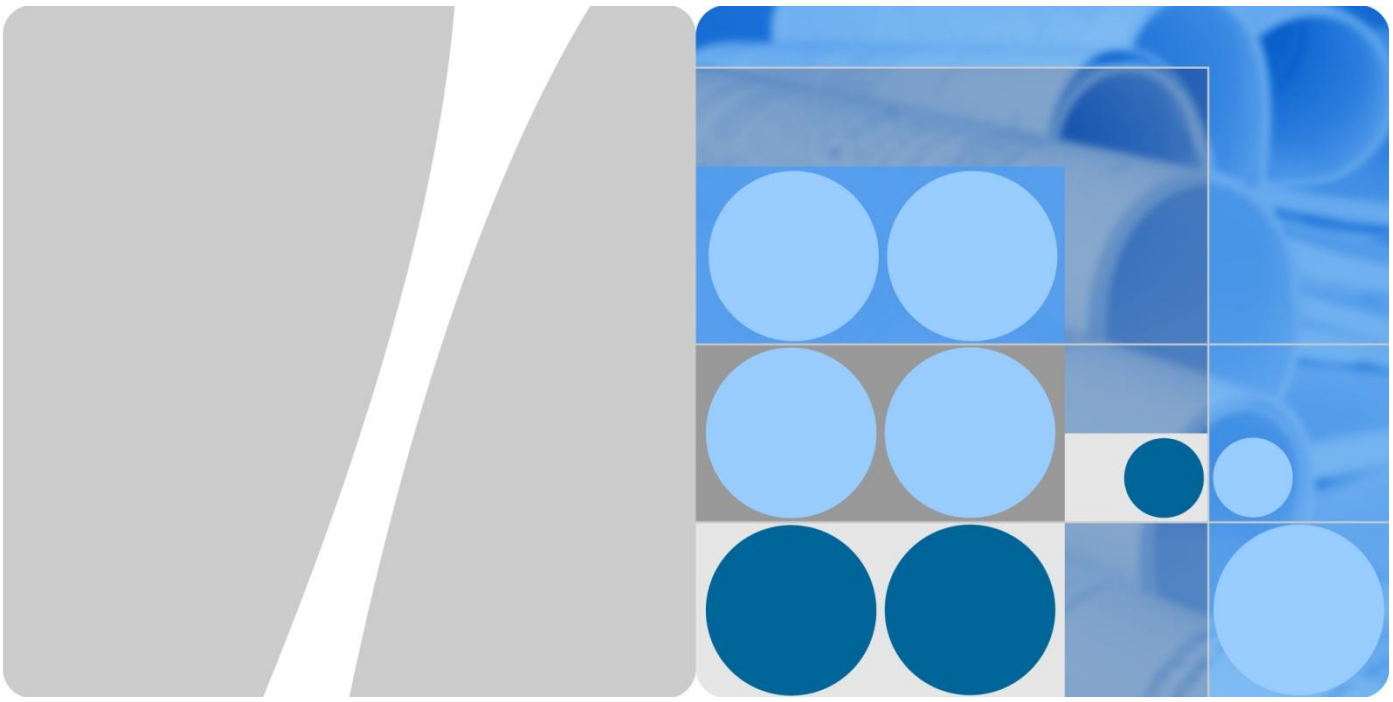
资料编码



eWBB 端到端加密解决方案白皮书

文档版本 v1.0

发布日期 2013-01-30~~2012-09-24~~

华为技术有限公司

商标声明

 和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

Contents

1 执行摘要

《eWBB 端到端加密解决方案白皮书》用于指导我司关于 eWBB 加密解决方案的说明。本文档重点描述华为 eWBB 加密解决方案的框架、原理、场景、特性、以及系统功能等方面，以让客户较为快速地理解方案讨论的范围、主要观点和结论。

2 方案概述

目前，移动通信技术已有广泛应用，但是移动终端的信号流没有经过加密处理，或者仅在无线传输部分进行加密处理。一些特殊的行业应用，例如军队、政府机关，需要移动通讯有更高的安全性，不仅要防止通讯内容在空口被监听，也要在陆地网络防止通讯被截获、监听等。为满足高安全性的通信需求，需要有基于移动交换网的端到端（E2E）加密通信系统。

华为 E2E 加密解决方案具有强大的加密功能

- 支持端到端语音全程加密
- 支持端到端语音半程加密

- 支持低速率（<1Mbsp）的数据加密，如文本文件、静止图像资料或较长的数据文件、IP 数据的加密
- 支持 PTT 加密
- 支持调度台加密
- 支持加密算法定制

华为 LTE E2E 安全通信方案先进的加密算法和合理的架构大大提高了用户通信的安全性，同时加密算法可以为用户定制，使用更放心。

3 网络架构

3.1 网络架构及网元

华为 LTE E2E 加密解决方案架构如 1 所示。

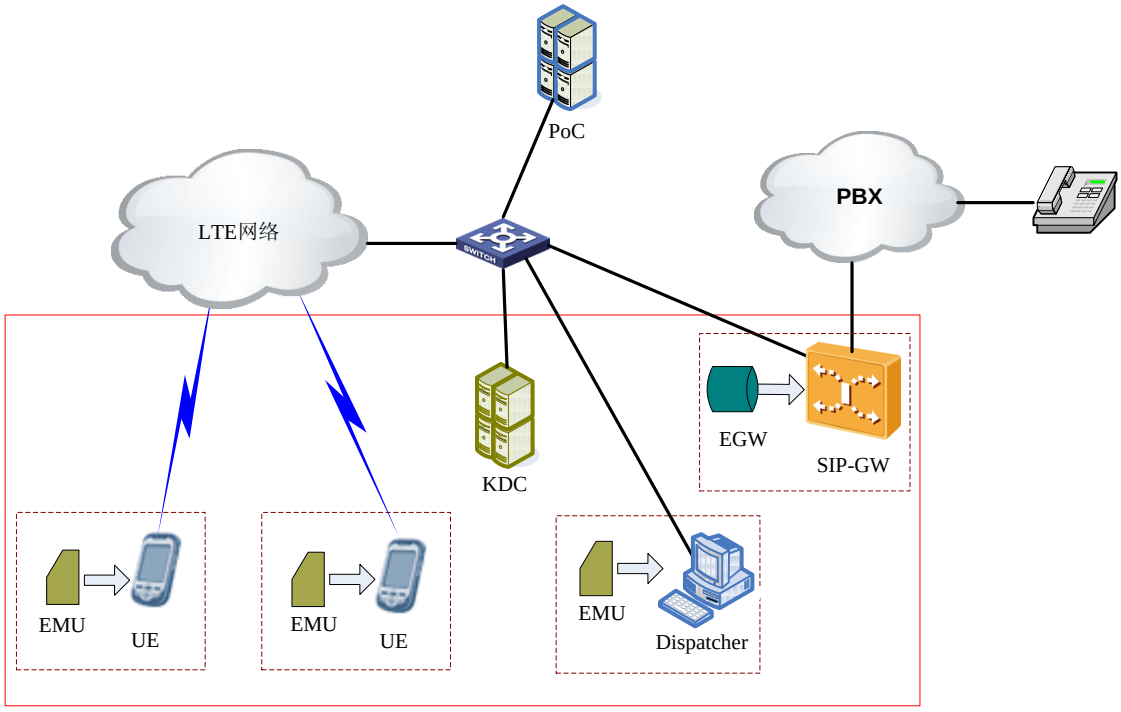


图 1 LTE E2E 加密解决方案组网

E2E 加密网络中的网元功能如下：

- 加密模块 EMU：插在加密终端上的 SD 卡，完成终端侧数据加解密处理。SD 卡一部分空间安装加密程序，另一部分空间做普通 SD 卡用。

- 加密终端：通过硬件加密/解密模块，对数字语音编码码流进行加解密。加密终端类型包括手持终端（T811、F811）和 CPE（T660、F660）。
- 加密网关 EGW：密码机，与 SIP 网关通过 RJ45 接口连接，完成 SIP 网关侧语音的加解密处理。
- SIP 网关 SIP-GW：完成 SIP 语音与普通电话语音的接续，通过加密网关 EGW 对语音加解密。
- Dispachter：PoC 集群调度台
- PoC：PoC 集群服务器。
- LTE 网络：加密业务对 LTE 网络是透明的。
- KDC：KDC负责密钥的管理和分发，单独的网元。

3.2 方案可获得性

加密特性涉及的网元

表 1 涉及的网元（集群）

UE	eNodeB	EPC	PoC Server	SIP-GW	KDC
√	-	-	√	O	√

表 2 涉及的网元（非集群）

UE	eNodeB	EPC	SIP-GW	KDC
√	-	-	O	√

说明

“√”表示涉及的网元。

“O”表示可选的网元。

3.3 网元配置及版本支持

表2 E2E Security解决方案配置

序号	网元	描述	备注
1	加密终端、加密模块	终端采用加密模块EMU，对语音、数据实现加解密	加密终端和加密模块配对使用，一个加密终端配一个加密模块。必配
2	eNodeB	eNodeB	必配，和加密特性无关
3	EPC	EPC	必配，和加密特性无关

4	PoC Server	PoC服务器。	可选，PoC服务器。
5	SIP-GW	SIP网关。	可选，SIP网关
6	KDC	KDC Version 1.0	必配，密钥分发中心。

说明

eNodeB、epc 的版本在本项目当中不作要求，建议使用配套的最新版本。

3.4 主要的网络接口与协议说明

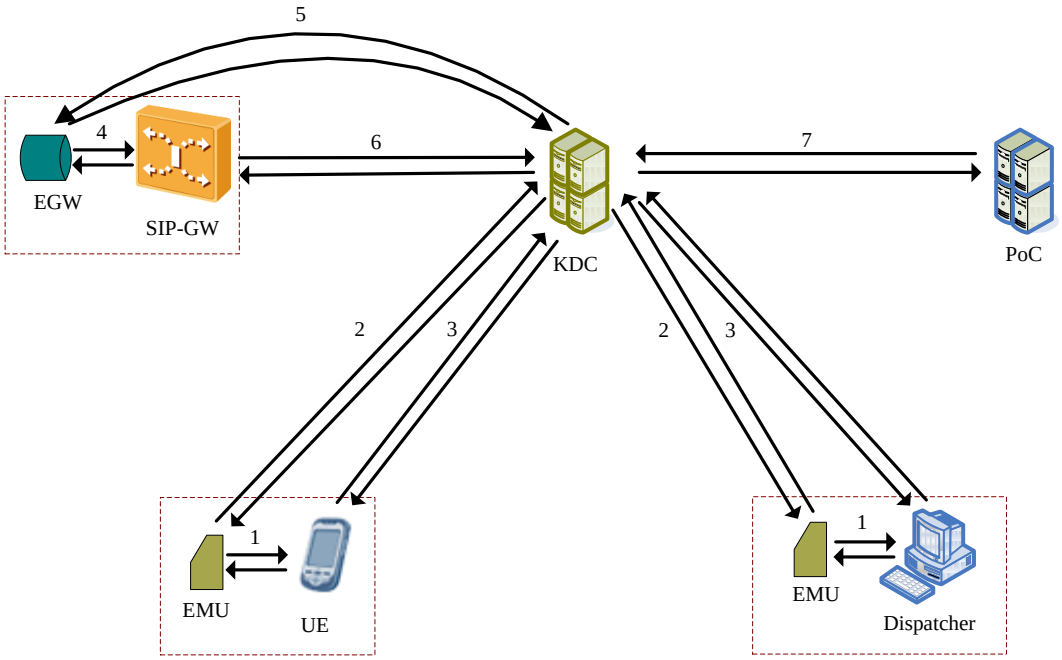


图 2 主要私有网络接口与协议

加密模块EMU与终端UE的接口：完成加密模块与终端的通信，私有接口

加密模块EMU与KDC的接口：完成加密模块与KDC的通信，私有接口

终端与KDC的接口：完成加密模块EMU与KDC之间的消息转发，私有接口

加密网关EGW与SIP-GW的接口：完成加密网关EGW与SIP-GW的的通信，私有接口

加密网关EGW与KDC的接口：完成加密网关EGW与KDC的的通信，私有接口

SIP-GW网关与KDC的接口：完成加密网关EGW与KDC之间的消息转发，私有接口

KDC和PoC的接口：完成PoC和KDC的通信，私有接口

4 加密算法及其实现过程

4.1 加密算法的基本分类

目前加密算法主要分成两类：对称加密算法和非对称加密算法。华为 E2E 加密方案中，同时采用了这两种加密算法相结合。例如，对称加密算法为：AES；非对称加密算法为 ECC。

在对称加密算法中，使用的密钥只有一个，发收信双方都使用这个密钥对数据进行加密和解密，这就要求解密方事先必须知道加密密钥。对称加密算法的特点是算法公开、计算量小、加密速度快、加密效率高。

非对称加密算法使用两把完全不同但又是完全匹配的一对钥匙：公钥和私钥。加密明文时采用公钥加密，解密密文时使用私钥才能完成，而且发信方（加密者）知道收信方的公钥，只有收信方（解密者）才是唯一知道自己私钥的人。采用非对称加密算法，收发信双方在通信之前，收信方必须获得收信方的公钥，而收信方拥有自己的私钥。由于非对称算法拥有两个密钥，因而特别适用于分布式系统中的数据加密。

4.2 对称加密算法

4.2.1.算法简介

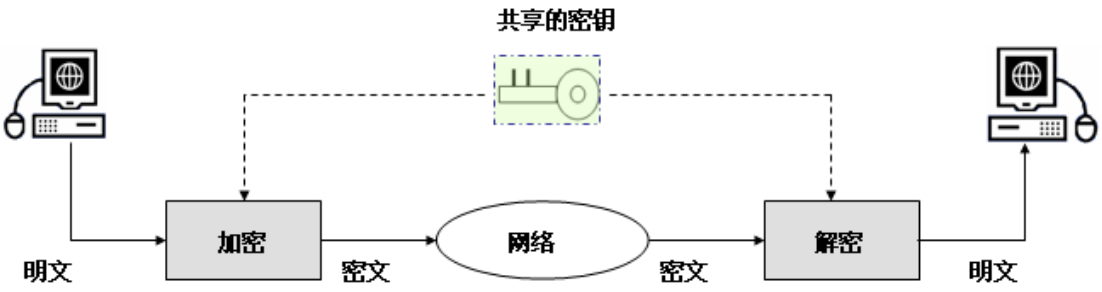


图 3 对称加密算法

对称加密算法使用相同的秘钥进行加解密，对报文加密花费的时间较少（与非对称加密算法相比），算法运算更有效。原因是这种秘钥较短。为此，对称加密算法用来对较长的报文进行加密和

解密。其特点是:密钥由发方(或第三方）产生,然后经一个安全可靠的途径送达收方(或双方），供解密使用。

目前流行对称加密算法有：DES，3DES，AES。下面详细介绍一下华为采用的 AES 算法。

4.2.2.AES 算法基本概念

AES, Advanced Encryption Standard,先介绍一下基本概念。

（1）State： 将需要加解密的文件读入内存,每次依次顺序截取其中的一个 Packet(128/192/256bit)分组进行处理,称为一个 *state* ,一个 *state* 是一个 4 ×Nb 矩阵,矩阵中的每个元素都是一个字节.Nb=Packet Length/32,所以 Nb 可以取值 4，6，8。

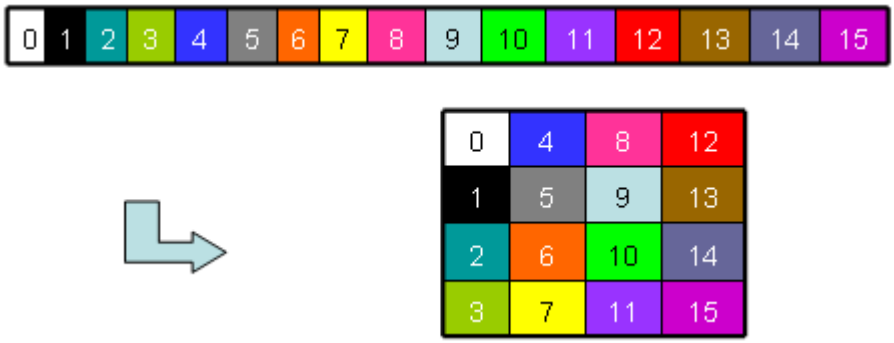


图 4 State

（2）Cipher Key: Cipher Key 也可以用一个 4 ×Nk 矩阵表示,矩阵中的每个元素都是一个字节。Nk=Key Length/32,所以 Nk 可以取值 4，6，8。

$K_{0,0}$	$K_{0,1}$	$K_{0,2}$	$K_{0,3}$
$K_{1,0}$	$K_{1,1}$	$K_{1,2}$	$K_{1,3}$
$K_{2,0}$	$K_{2,1}$	$K_{2,2}$	$K_{2,3}$
$K_{3,0}$	$K_{3,1}$	$K_{3,2}$	$K_{3,3}$

Nk = 4
Key Length = 128 bits

图 5 Key

（3）**Round：**

Round 指加密的轮数，用 Nr 表示,Nr 的取值和 Packet Length，Key Length 有关。

Round (Nr)	Packet Length=128	Packet Length=192	Packet Length=256
Key Length=128	10	12	14
Key Length=192	12	12	14
Key Length=256	14	14	14

Round 也指轮变换，也即通过每轮的加密进行变换。除最后一次外轮变换都需要经过 4 步。以下是轮变换的基本过程。

Standard Round

```
Round (State, RoundKey)
{
    ByteSubstitution;     // step 1
    ByteRotation;         // step 2
    MixColumn;            // step 3
    AddRounKey;           // step 4
}
```

Final Round

```
FinalRound (State, RoundKey)
{
    ByteSubstituion;
    ByteRotation;
    AddRoundKey;
}
```

4.2.3.AES 算法加解密流程

流程中最关键的是方框内的轮变换过程。至于其他的在 4.2.2 中已经有描述。所以这里就介绍轮变换的实现过程。

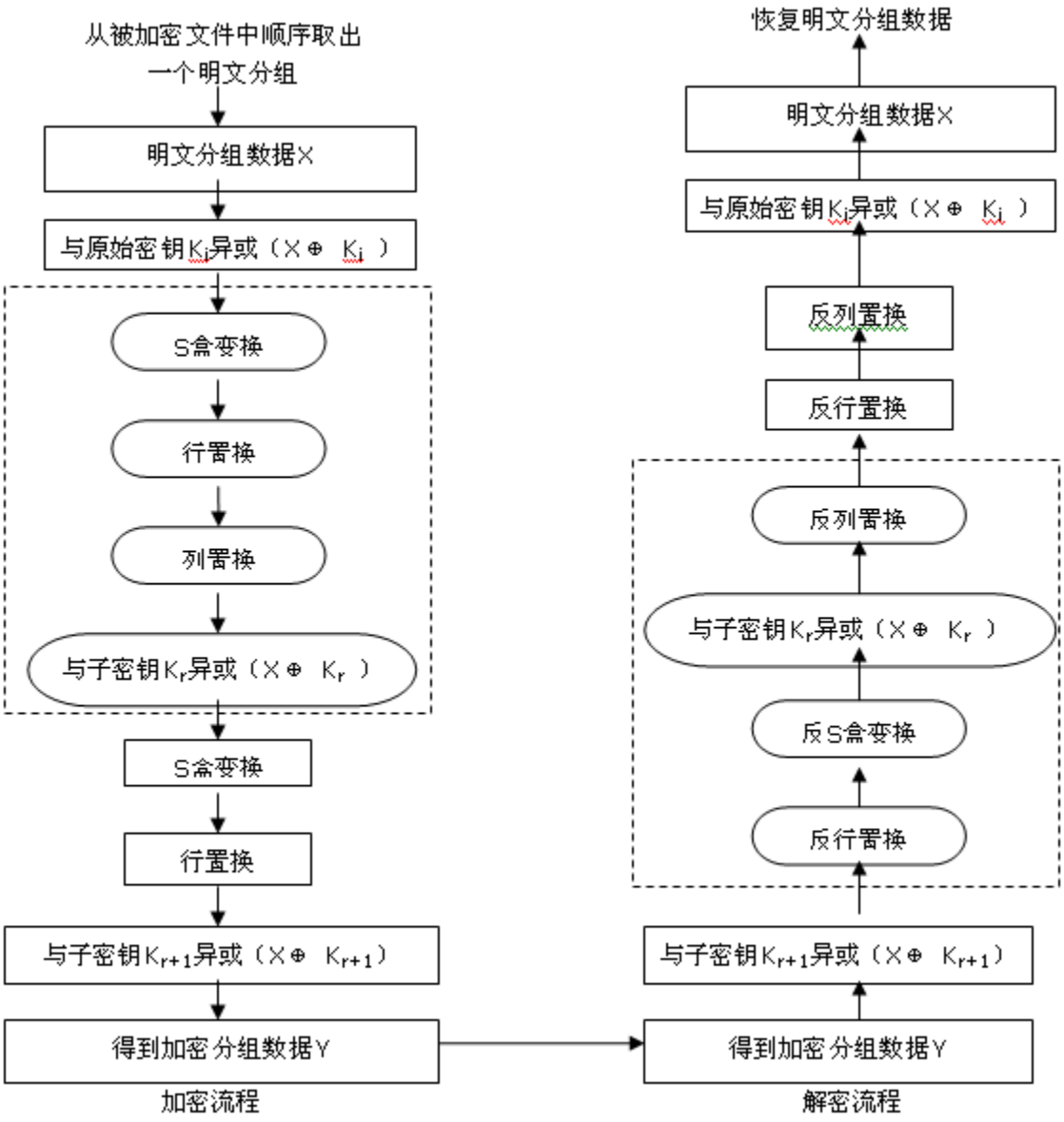


图 6 AES 加解密流程

（1）ByteSubstitution（称为 S 盒）

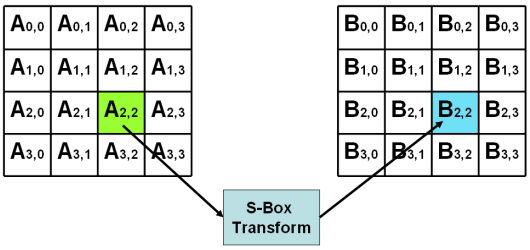


图 7 S 盒变换

（2）ByteRotation（称为行置换）

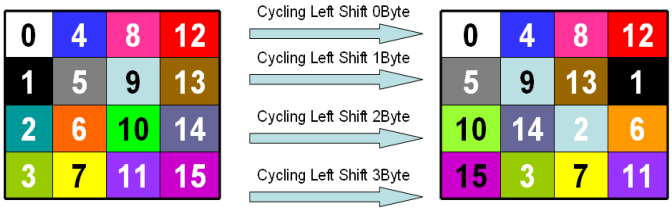


图 8 行置换

（3）MixColumn（称为列置换）

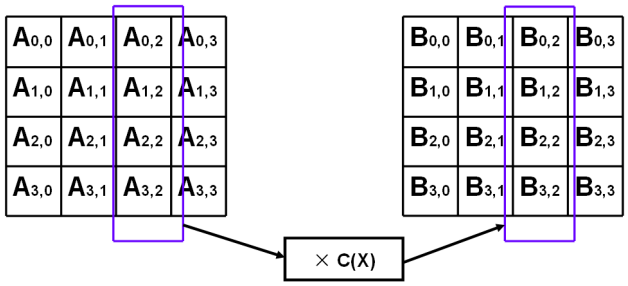


图 9 列置换

（4）AddRoundKey（与子密钥进行异或运算）

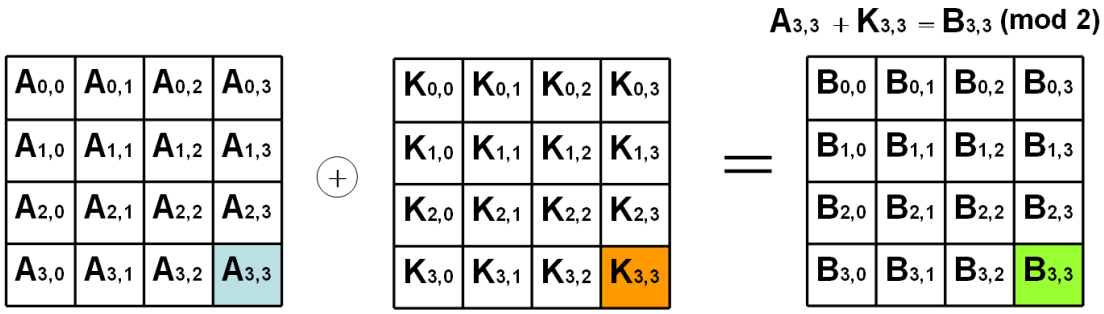


图 10 与子密钥进行异或运算

4.3 非对称加密算法

4.3.1.算法简介

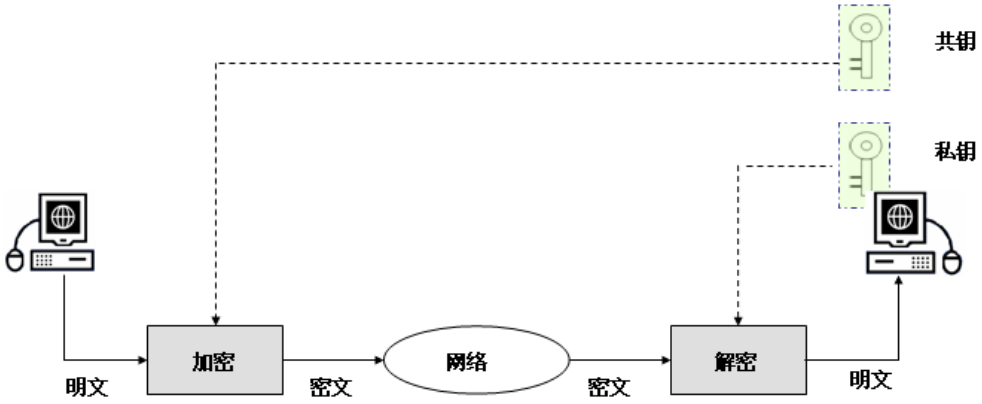


图 11　非对称加密算法

非对称加密算法使用公钥加密，私钥解密。

非对称加密算法较为复杂，运算时间长；对短报文更加有效；非对称加密算法中，共钥拥有者和它的共钥的关联必须被验证；目前流行的非对称加密算法有：RSA，DSA，ECC。

4.3.2.ECC 算法加解密流程

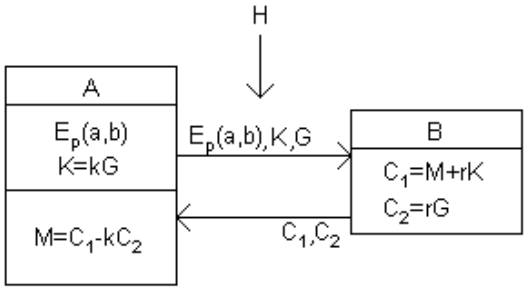


图 12 非对称加密算法流程

1、用户A选定一条椭圆曲线Ep(a,b)，并取椭圆曲线上一点，作为基点G。

2、用户A选择一个私有密钥k，并生成公开密钥K=kG。

3、用户A将Ep(a,b)和点K，G传给用户B。

4、用户B接到信息后，产生一个随机整数r。

5、用户B计算点C1=M+rK；C2=rG。

6、用户B将C1、C2传给用户A。

7、用户A接到信息后，计算C1-kC2，结果就是点M。因为C1-kC2=M+rK-k(rG)=M+rK-r(kG)=M，再对点M进行解码就可以得到明文。

4.4 密钥管理

E2E 加密安全性的保障很大程度上取决于密钥的管理；华为安全通信方案采取以下安全措施：

- 密钥由 KDC 集中管理。
- 使用加密功能必须在 KDC 开户。
- 终端使用加密功能前必须和 KDC 双向认证。
- 密钥周期更新，可配。

表 5 密钥管理场景划分

序号	场景描述
1	KDC、加密模块密钥管理
2	终端开机认证
3	加密模块状态查询
4	KEK 更新（二级密钥，例如对语音密钥做加密的密钥）

4.5 加密算法实现系统介绍

4.4.1.KDC

KDC, Key Distribution Center，负责密钥的管理和分发。

1.硬件系统

图 13 KDC 物理结构

硬件系统就是一台IBM 公司生产的System x3650 Type 7979 型服务器，密钥管理系统（KDC）安装在服务器中。具体性能参数、安装指南等参考产品说明书。

服务器长宽高分别为698 毫米×443.6 毫米×85.4 毫米。

2.KDC 软件系统

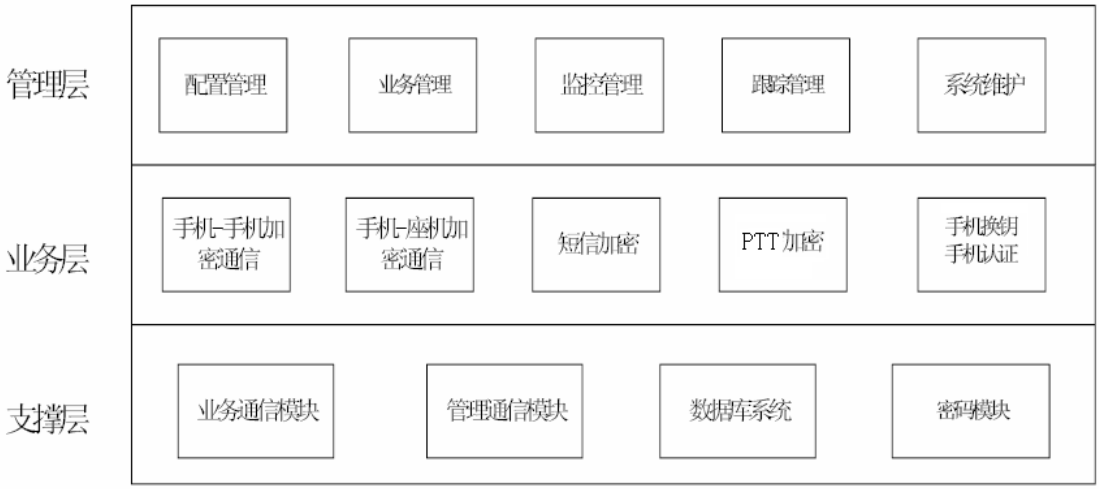


图 14 KDC 软件结构

共分 3 个层次：

- 支撑层：是实现整个业务的基础。包括业务通信模块，管理通信模块，数据库系统以及密码管理模块；
- 业务层：实现各种加密业务应用。具体业务场景第4节。
- 管理层：这里主要是客户端软件，见图19，实现各种消息跟踪、配置操作、维护操作等。

4.4.2.UE

在终端中增加加密模块 EMU 实现加解密。以下是终端的基本参数。

表 4 终端基本参数

Item	Description
Type	Bar-type
Display	l Size: 4.5 inches l Type: TFT IPS touchscreen l Color: 16M colors l Resolution: 1280 x 720 pixels
Dimensions (H x W x D)	146 mm x 72 mm x 21 mm
Weight	300 g (with battery)
Technical standard	3GPP LTE R8
Working band	1.8 GHz LTE TDD (1785 MHz to 1805 MHz) （可定制）
Data services	LTE TDD 2UL: 2DL l Downlink: up to 68Mbps l Uplink: up to 17Mbps
SIM card	Standard 6-pin SIM card port. Does not support hot swapping.
Port	Standard micro USB port, microSD card slot, and 3.5 mm headset jack
Storage capacity	l ROM: 4 GB l RAM: 1 GB
Extended storage space	microSD card (up to 32 GB)
Processor	TI OMAP4460 1.5 G + LTE MODEM
Device control	Touch buttons, power key, volume keys, PTT key, and emergency dial key.
GPS	GPS/AGPS/SUPL1.0/Glonass

Temperature	l Operating temperature: –20 ℃ to +55 ℃ l Storage temperature: –40 ℃ to +70 ℃
Battery	l Type: Li-ion battery l Capacity: 2600 mAh
Operating humidity	5% to 95% RH
Camera	l Rear camera: 8 MP AF full HD l Front camera: 1.3 MP HD
Radio	Built-in radio
Bluetooth	Bluetooth 3.0
Antenna	Built-in antenna
Wi-Fi	802.11b/g/n. Also functions as a Wi-Fi hotspot.
USB	USB 2.0 480 Mbit/s
Maximum transmit power	23 dBm (±2)
RF sensitivity	–94 dBm/20 MHz –100 dBm/5 MHz –97 dBm/10 MHz
Sensor	Accelerometer Light sensor Tilt sensor Proximity sensor

表 5 加密模块参数

加密模块	支持AES、ECC等算法 支持语音加密 支持数据加密 支持用户认证

5 业务场景

5.1 UE-UE加密通话

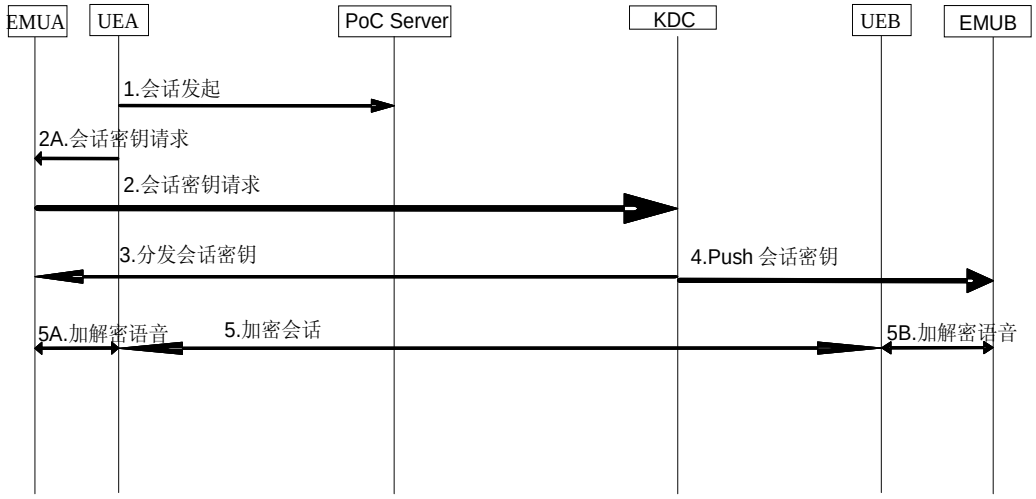


图 15 UE-UE 加密通话流程

1. 主叫 SIP 应用发起 SIP 会话

2. 主叫用户选择加密功能后，主叫向 KDC 发起密钥分发请求。

3. KDC 收到密钥分发请求后向主叫分发密钥，同时向被叫 Push 密钥。

4. 主叫收到 KDC 分发的密钥后，将需要加密的语音发送给加密模块。

5. 加密模块将加密后的语音发送用户 A，用户 A 向用户 B 发送语音。

6. 用户 B 将收到的加密后的语音发送给加密模块。

7. 加密模块对语音解密后返回给用户 B。

5.2 UE-PBX加密通话

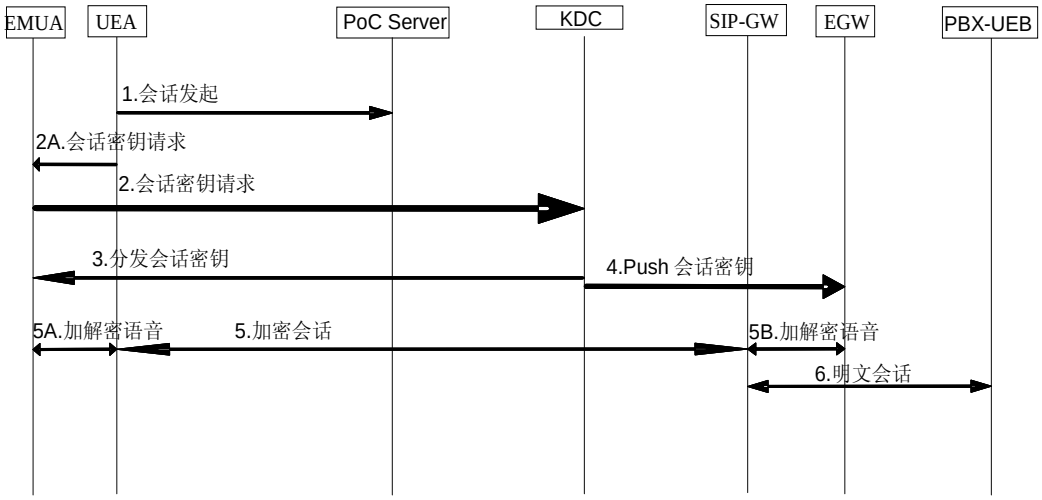


图 16 UE-PBX 加密通话流程

1. 主叫 SIP 应用发起 SIP 会话

2. 主叫用户选择加密功能后，主叫向 KDC 发起密钥分发请求。

3. KDC 收到密钥分发请求后请主叫分发密钥，同时向 SIP 网关 Push 密钥。

4. 主叫收到 KDC 分发的密钥后，将需要加密的语音发送给加密模块。

5. 加密模块将加密后的语音发送用户 A，用户 A 向 SIP 网关发送语音。

6. SIP 网关将收到的加密后的语音发送给加密网关。

7. 加密网关对语音解密后返回给 SIP 网关。

8. SIP 网关转发解密后的语音到 PBX 网络。

5.3 组呼加密

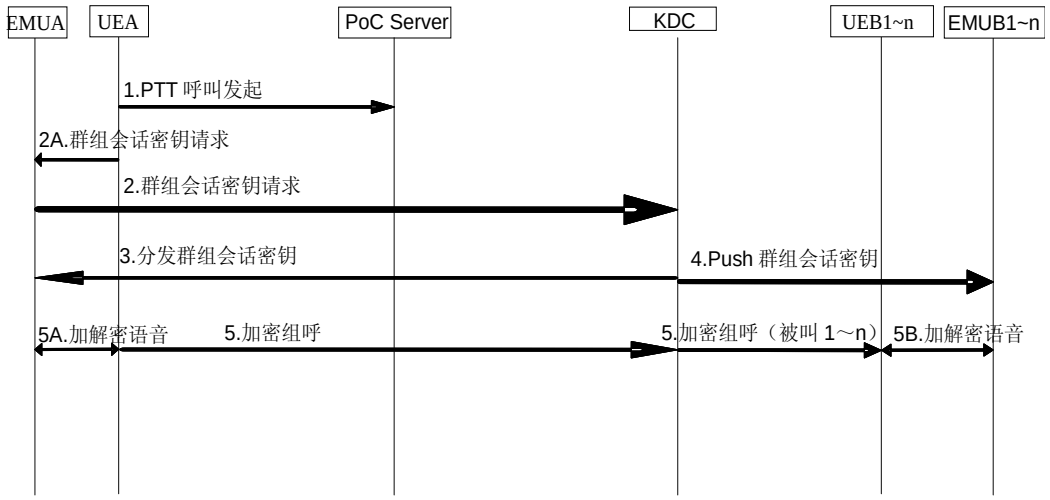


图 17 PTT 加密通话场景

1. 用户按 PTT 键发起组呼呼叫消息与非加密呼叫相同，如果用户选择加密功能，用户 A 向 KDC 请求群组会话密钥
2. KDC 收到用户 A 的群组会话请求 7，生成群组会话密钥，向用户 A 分发群组会话密钥，同时向群组所有被叫用户 Push 群组会话密钥
3. 呼叫建立同已有 PTT 呼叫流程
4. 被叫接入流程同已有 PTT 呼叫流程
5. 群组用户收到群组会话密钥后，加密语音通话

说明

1.以上以 PTT 中普通群呼为例。PTT 中某两个 UE 之间的呼叫流程基本同语音呼叫。

5.4 数据加密

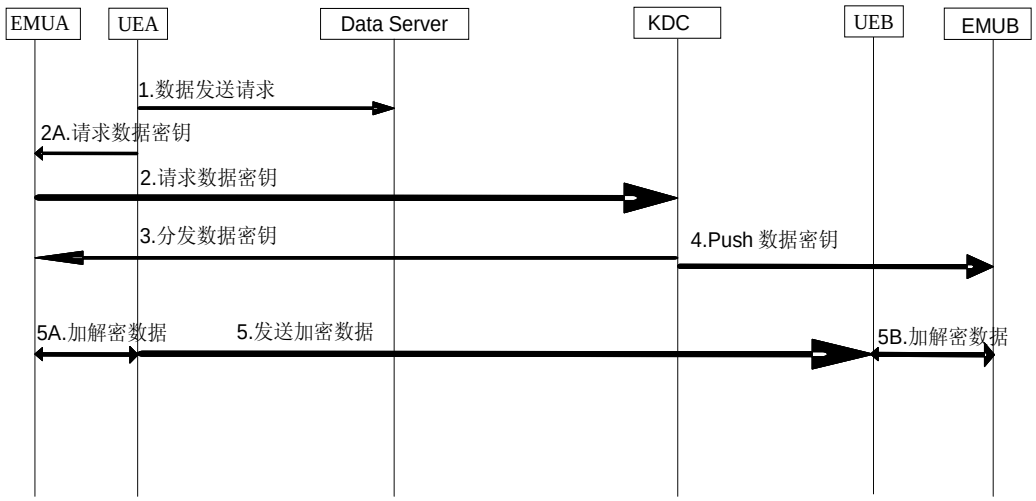


图 18 数据包加密流程

1. 用户 A 向用户 B 发送数据包，发送之前向 KDC 发起数据密钥分发请求

2. KDC 收到用户 A 的数据密钥分发请求后，生成数据密钥，向用户 A 分发数据密钥，同时向用户 B Push 数据密钥

3. 用户 A 收到 KDC 的数据密钥后，将需要加密的数据包内容发送给加密模块。

4. 加密模块将加密后的数据包内容发送用户 A，用户 A 向用户 B 发短数据包。

5. 用户 B 将收到的加密后的数据包发送给加密模块。

6. 加密模块对数据包解密后返回给用户 B。

5.5 加密通话中的移动性

加密通话中，用户从一个地方移动到另一个地方，加密特性继承 LTE 既有的切换功能，用户的移动不会导致掉话。

加密通话中的移动性与普通语音流程切换流程相同。

5.6 加密算法替换

5.6.1.算法替换种类

由于 LTE 加密系统中语音和数据加密都采用对称算法，所以系统只提供对称算法的替换，不支持非对称算法的替换。

5.6.2.算法替换的实体

在加密系统中，涉及算法的实体包括 KDC、手机密码模块和加密网关的密码模块，它们是相互关联的，其中一方替换，其它两方必须做相应的替换，否则就不能互联互通。

5.6.3.算法替换的实现要求

对称算法的替换支持分组长度为 256bit 对称算法的替换，客户可以通过算法定制的功能，自行刷新算法的同时修改密钥的长度。算法加密后的密文要求与原文长度相等；当原文不足一个分组时，进行加密运算后不能补位。

5.6.4.算法替换的实现过程

（1）KDC 部分算法替换

提供密钥生成函数，及相关接口要求；客户在他们的加密算法中调用这些接口函数以实现整个密钥的生产；替换算法函数以动态库方式导入到 KDC 中，被加载运行。我们提供接口标准、编译环境和更新操作指导。

（2）手机密码模块部分算法替换要求

手机密码模块只提供对称算法核心替换，语音数据加密功能由密码模块本身处理；

手机密码模块将提供基于命令行的编译连接器、程序代码框架，算法调试环境由用户自行提供，算法采用 C 语言实现；

用户将扩展的算法核心通过编译连接器编译成目标代码后，通过写卡器将算法核心下载到手机密码模块中（目标代码的下载可通过 KDC 的管理客户端在手机用户开户时写入）；

输入输出接口要求、编译环境要求、代码框架文档在后续的算法替换文档中提供。

（3）加密网关中的部分算法替换要求

提供非对称加密算法 lib 库。

同时提供对称算法的加密和解密函数接口要求，该部分的加密和解密函数实现整个加解密和数据封装过程。客户根据上述接口要求开发他们的对称加密算法 c 文件。然后在提供的编译环境中客户生成对称加密算法 lib。

按照操作手册把非对称加密算法 lib 库和对称加密算法 lib 库结合起来供加密网关使用。

在加密网关上的替换算法，在采用相同明文、密钥的情况下，其运算结果要求能与手机密码模块中语音加密运算结果相同，否则加密业务不能正常运。

6 方案优势

6.1 业务受益

主要针对政府部门、军队的专网，有效保护信息安全，使客户避免由于泄密造成的各种损失。

6.2 加密性能

华为 LTE E2E 解决方案加密性能如下：

- 非对称加密算法，可实现 ECC 加密算法，KDC 和手机密码的 ECC 密钥长度为 192bit。
- 对称加密算法，安全性和加密强度方面与 AES 算法同等水平。KEK 和会话密钥 sessionkey 长度为 256bit。
- 客户可以通过算法定制的功能，自行刷新算法的同时修改密钥的长度。
- 加密、解密的算法可以由用户写入，即算法可以更新。

KDC 和终端加密模块的加密性能指标如下：

表 6　KDC 主要性能指标

参数名	指标
最大用户数	2 万
处理分发时间	< 400ms
加密呼叫成功率	> 99.7%

表 7 终端加密模块主要性能指标

参数名	指标
单次加解密时间	< 5ms
通话功耗	< 40mah
待机功耗	0
语音时延	< 10ms

6.3 方案特点

- 端到端全程加密，全程有效保护信息安全。
- 双向认证机制，开机时 KDC 和终端互相严格身份认证。
- 硬件加解密，终端通过硬件加密/解密模块，在话音经过数字语音编码之后对编码码流进行加密，从而实现对语音的加密。在接收端通过在话音解码器之前先送入硬件加密/解密模块实现解密。
- 速度快，延时小，不影响语音质量。
- 算法定制，提供定制接口和规范，客户使用更自由，更放心。
- 对称/非对称加密算法同时使用，有效保证信息安全。
- 密钥管理，由 KDC 统一管理，一话一密，支持秘钥备份、更新。方便，有效。
- 易于实施：组网简单，只需添加新的网元 KDC，同时终端采用加密模块；实施方便；成本优势明显，性价比高。
- 可靠性方案，KDC 双机备份。

7 缩略语表

附录1：缩略语

缩略语	英文	中文
PBX	Private Branch Exchange	用户级交换机
KDC	Key Distributor Center	密钥分发中心
KEK	Key Encryption Key	加密密钥的密钥