Chapter5 ：

Security in Bluetooth® Networks and Communications

无线个域网安全技术

1023041121杜宏煜

INTRO.

PART.1 发展历程与技术基础

HISTORY & TECH BASIS

ATTACK.

PART.4 安全攻击与防御措施

ATTACK & DEFENSE

APPLY.

PART.2 组网结构

NETWORK STRUCTURE

SECURITY.

PART.3 安全目标与四种安全模式

SECURITY GOAL & SECURITY MODES

蓝牙作为一种短距离无线通讯技术，可以在不依赖互联网或局域网等其他类型的网络的条件下，支持所有安装了蓝牙软硬件模块的设备之间进行简单即时的连接和数据交换。

这样的特性也为蓝牙技术带来了丰富的应用场景，智能手机，无线耳机，智能音箱，个人电脑，Airdrop，共享单车等都是蓝牙技术方便人们生活的体现。

Time

1994

1994 年，爱立信移动通信公司的一个研究小组启动了一项关于通用短程低功耗无线连接的可行性的研究，该技术主要用于移动电话、耳机、车载设备和计算机之间的数据交换。

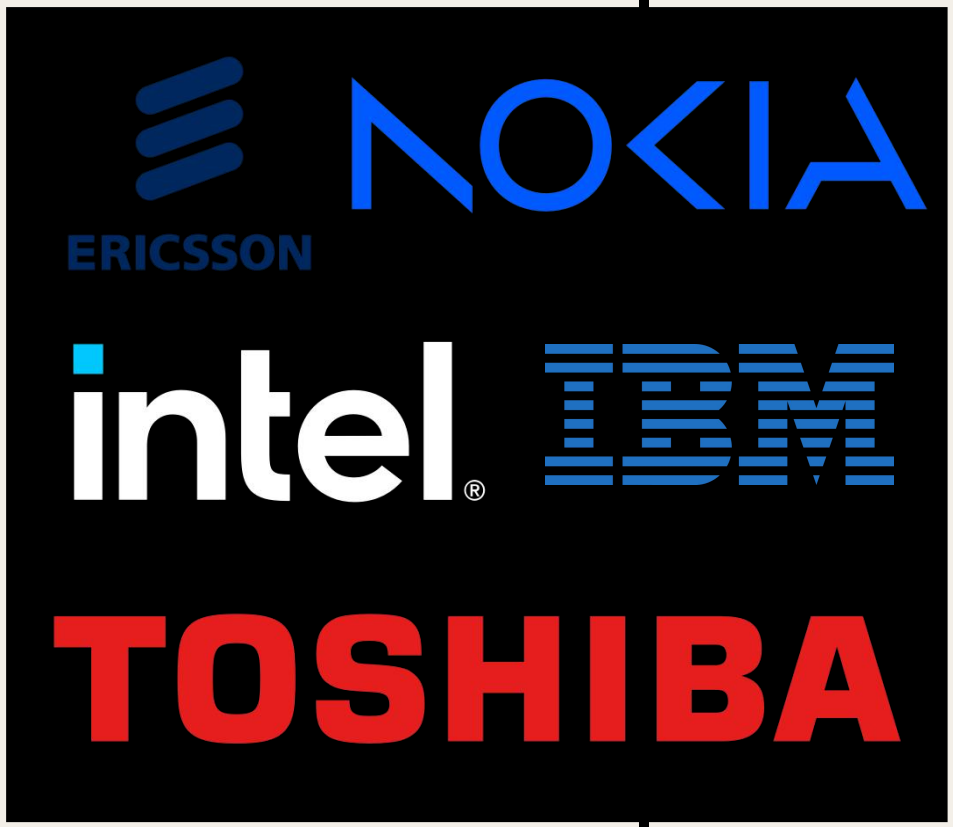
发明者希望为设备间的通信创造一组统一规则（标准化协议），以解决用户间互不兼容的移动电子设备。这也是后来该技术得名蓝牙的原因。

“Bluetooth”一词是斯堪的纳维亚语言词汇Blåtand/Blåtann的英语化。这个词的来源是10世纪丹麦和挪威国王蓝牙哈拉尔。蓝牙哈拉尔曾统一了因宗教战争和领土争议而分裂的挪威和丹麦，因此蓝牙技术的研发小组以其名号期许新技术能集成各大品牌的标准。

Time

1998/1999

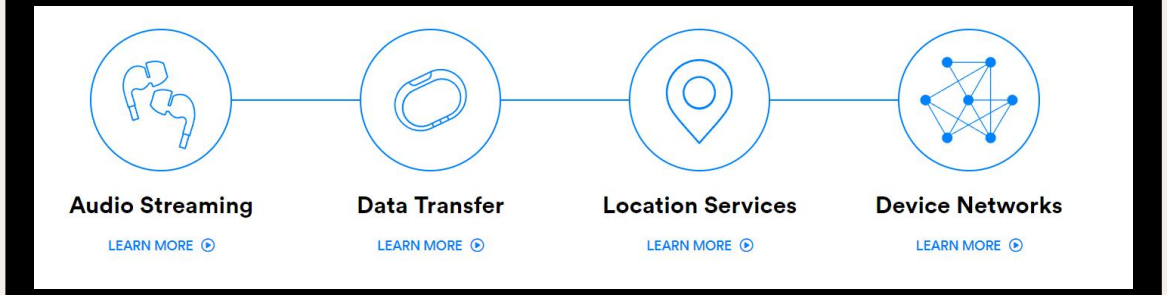
四年后，一个名为蓝牙特别兴趣小组(SIG, Bluetooth Special Interest Group)成立，创始成员包括爱立信、诺基亚、英特尔、IBM 和东芝。



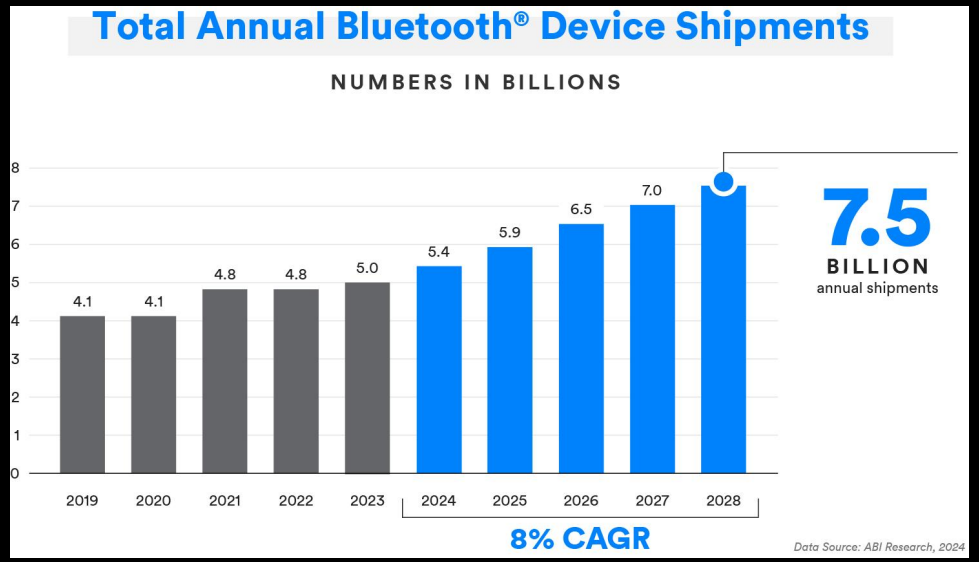
一年后，蓝牙1.0版本发布，1.0 版本存在许多问题，制造商很难使其产品实现互操作(没有实现最初的宗旨)。1.0 版还在连接过程中强制传输蓝牙硬件设备地址(BD_ADDR)，导致在协议层面无法实现匿名，其传输速率仅有732.2 kbit/s–2.1 Mbit/s(not KB or MB)，无法实现音乐播放功能。

Time

随着时间的推移和SIG小组的持续研究，蓝牙技术不断发展，时至今日已经发布了5.4版本，具有如低功耗，高速率数据传输，多设备连接和安全性保证等诸多优秀的特性。



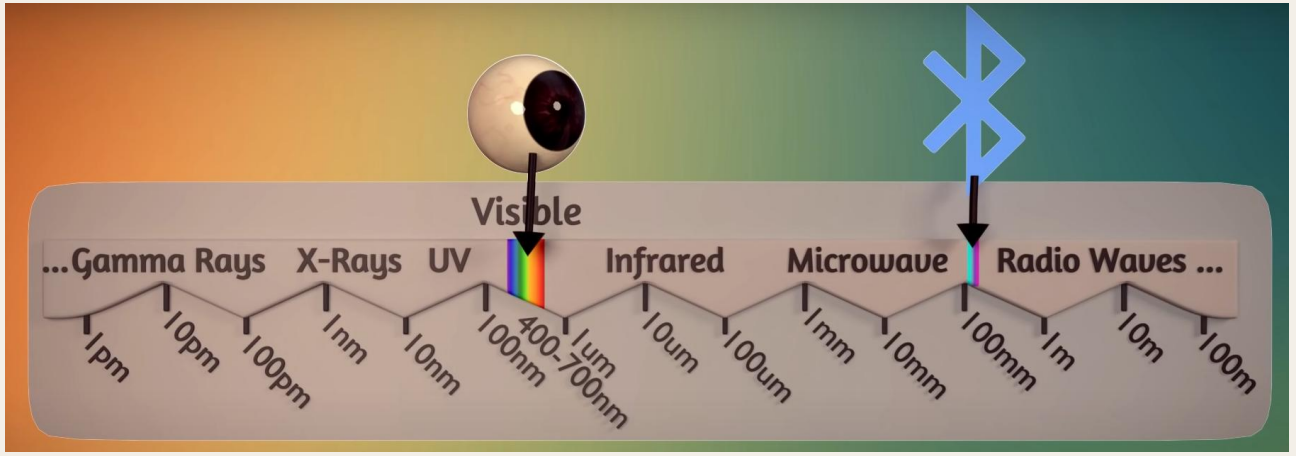
目前，蓝牙特别兴趣小组（Bluetooth SIG）在电信、网络、计算和消费电子领域拥有超过一万五千家会员公司。蓝牙模块集成在大多数智能手机、无线耳机以及许多新发布的笔记本电脑和格式各样的计算设备中。随着物联网(IoT)、智能家居、智能汽车的发展，蓝牙的应用场景仍在不断拓宽。

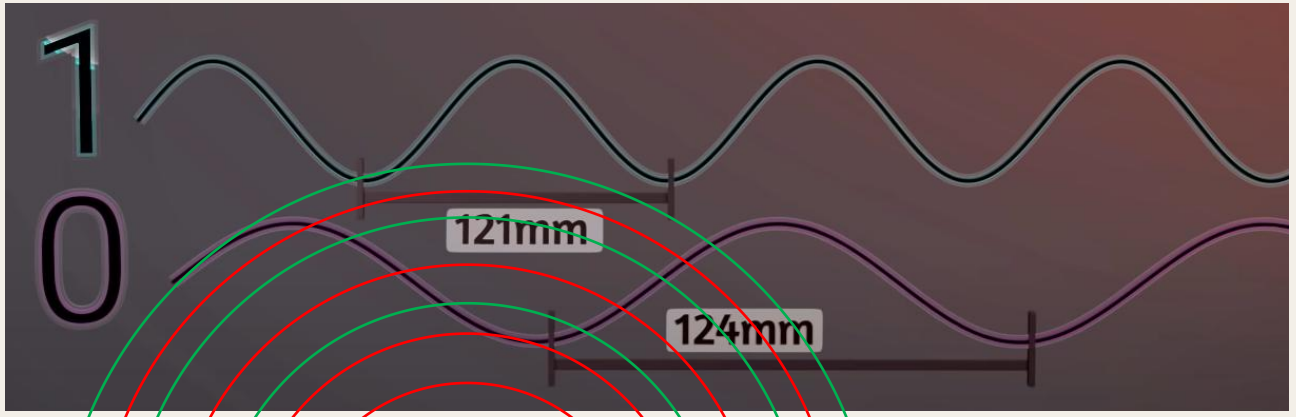


Today

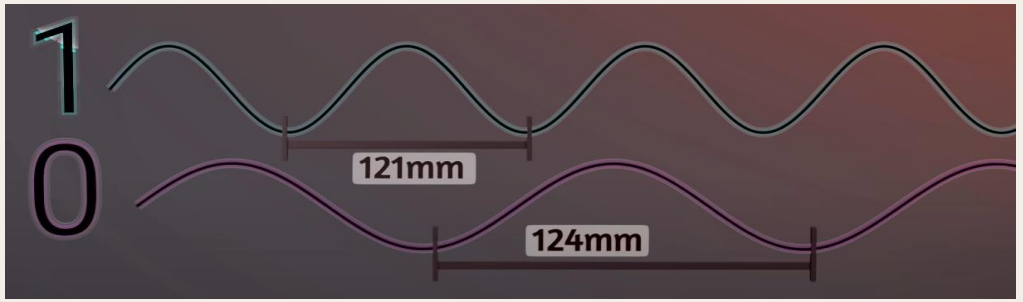
PART.1 发展历程与技术基础：工作原理

1111110110101101010111000111……



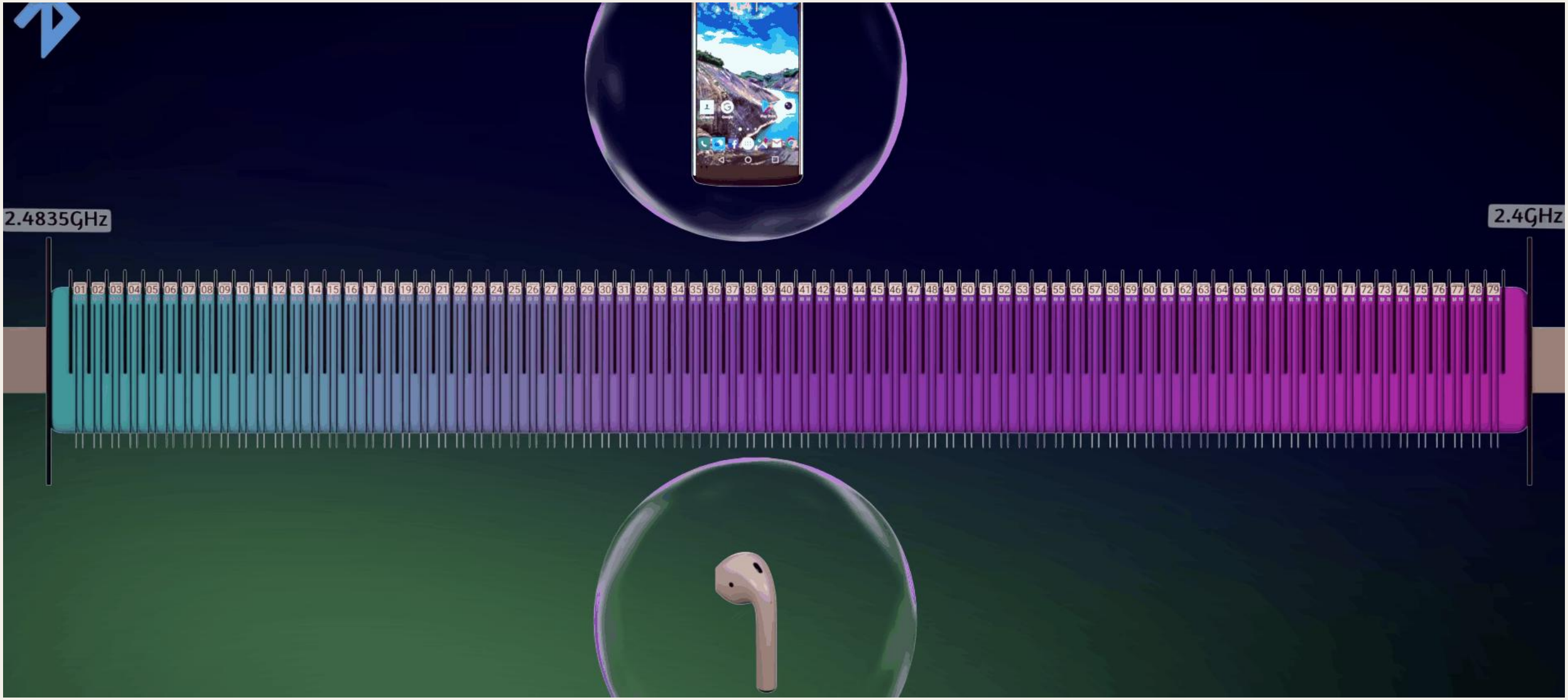


与IEEE 802.11b/g WLAN和许多其他无线通信技术一样，蓝牙在2.4 GHz ISM射频频段上工作。所以该通讯频段上非常拥挤。为了减少在如此拥挤的频谱段中信号干扰，蓝牙在通信中使用了跳频扩展频谱（FHSS）技术。蓝牙在79个不同的无线电信道上运行，能够以每秒1600次的频率跳频传输数据和语音，每秒3200次的频率跳频进行信令。每个信道上的驻留时间为625微秒。考虑到实现频率切换和控制交换需要259微秒，蓝牙可以在每帧期间传输数据366微秒。蓝牙允许1时隙、3时隙和5时隙帧。假设带宽为1 MHz且每赫兹1比特，1时隙帧的数据传输速率为366 bps，3时隙帧为1.616 Kbps，5时隙帧为2.866 Kbps。FHSS不仅降低了蓝牙信号被其他信号干扰的机会，还通过不断变化频率提供了一定程度的传输安全性。这使得恶意节点更难找到正在使用的确切频率，从而更难窃听通信数据。



2.4 GHz = 124.9135241667 mm

PART.1 发展历程与技术基础：工作频率



海蒂·拉玛

Hedy Lamarr

电影明星

“跳频扩频之母”

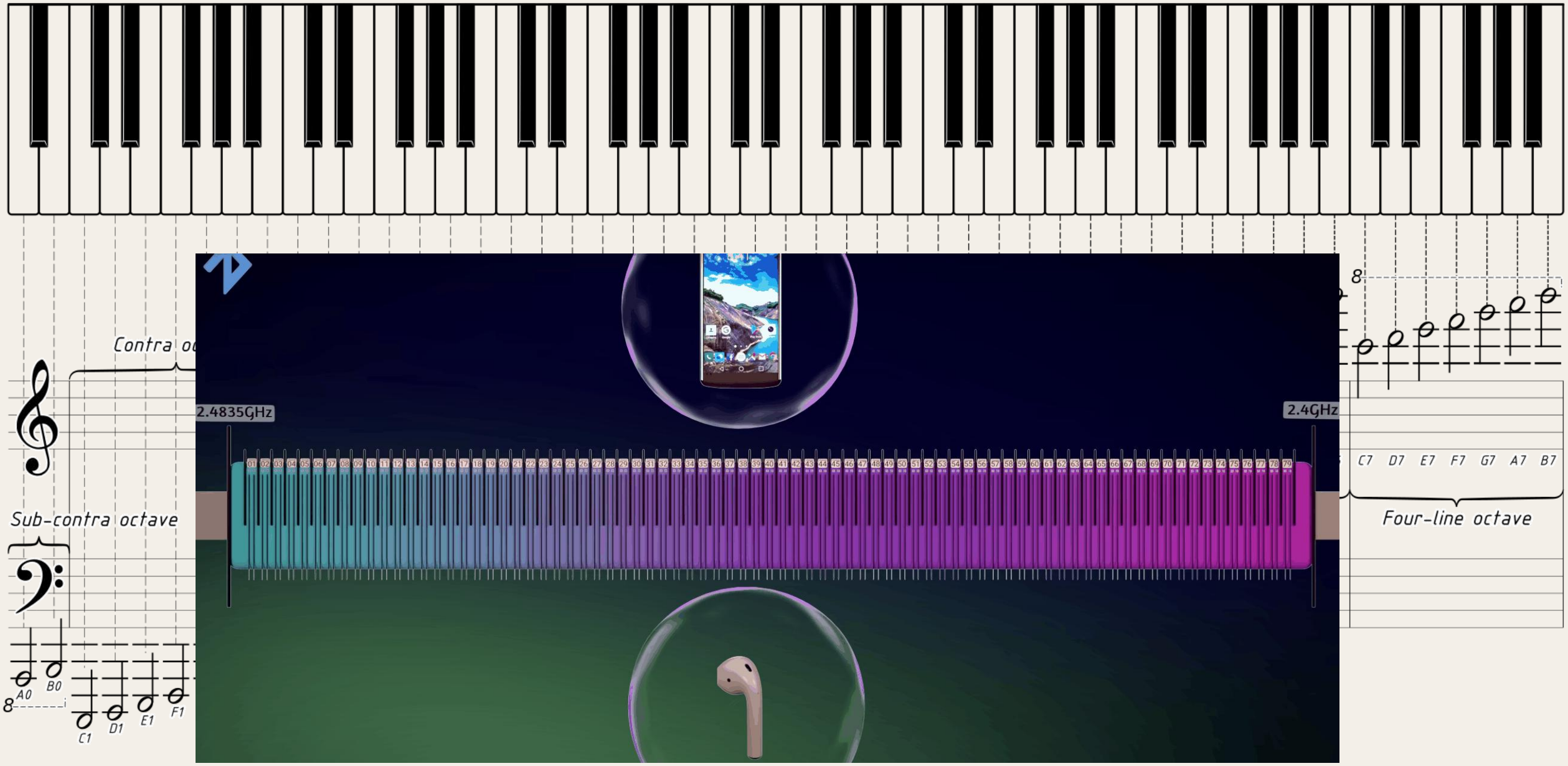
乔治·安太尔

George Antheil

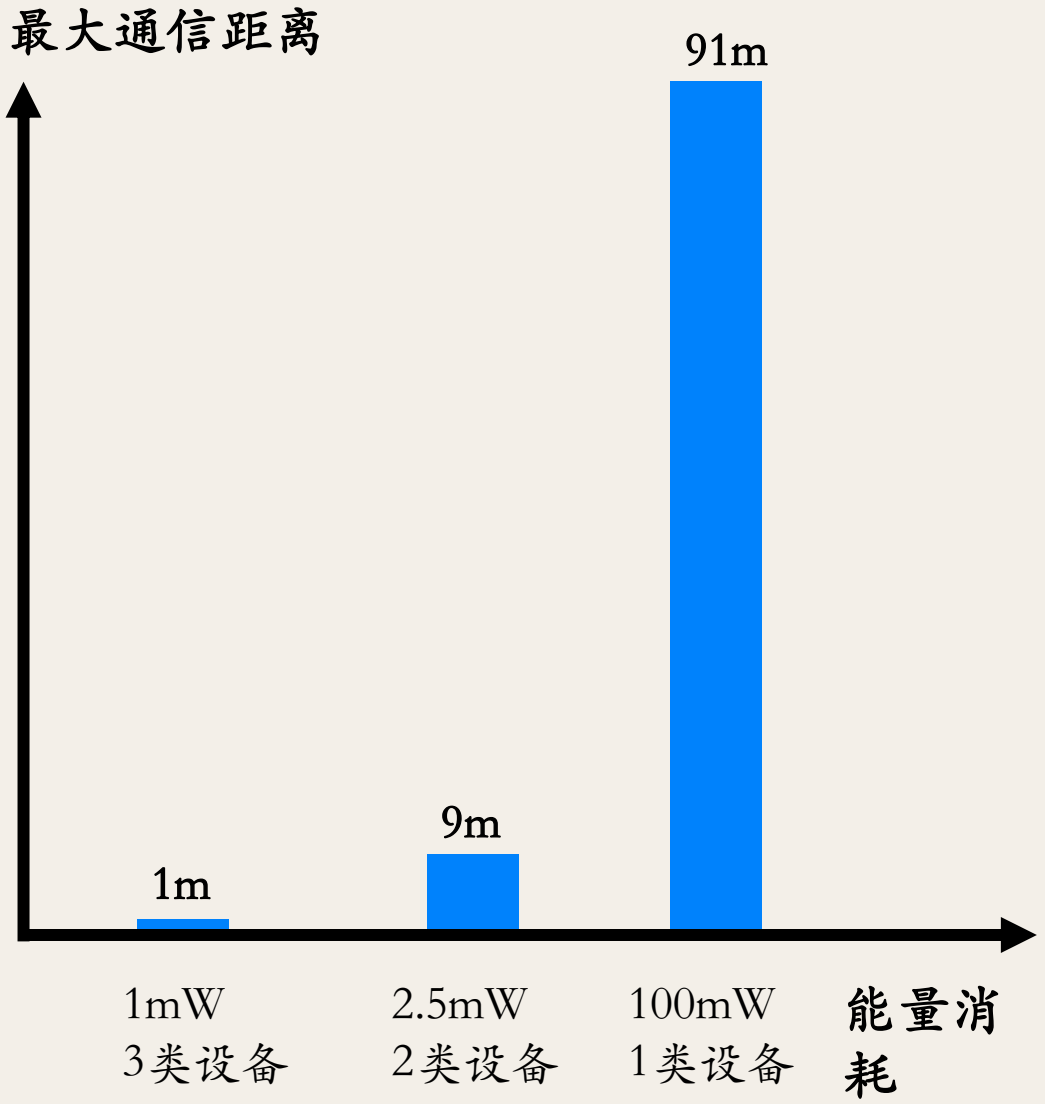
钢琴家

1940年夏天（二战期间），拉玛在一个聚会上认识了从德国移民的钢琴家乔治·安塞尔。拉玛把安塞尔邀请到家中，询问通过调节内分泌进行塑身的问题。但是他们的讨论转到了更重要的话题，拉玛想起自己在一次晚宴上和第一任丈夫（腰缠万贯的奥地利军火商）生活的时期，她曾听到官员们谈起如何操纵鱼雷的内容。如果是直接使用遥控则很容易被相同频率的信号干扰从而使鱼雷失去目标。某个下午安塞尔漫不经心地弹着钢琴，拉玛想到如果改变键盘可以改变声音，那么改变无线电信号频率同样可以改变信号。而安塞尔则想衍生出具体的实施方法，他曾经在1926年的《机械芭蕾》中使用了16架自动演奏钢琴，这些钢琴由滚筒驱动。当在鱼雷的接收器和舰上船的发射器内部安装有相同编码的读写器，让两者同时运转时，时钟调整频率，就可以完成这种跳频扩频，使敌人难以操控。

PART.1 发展历程与技术基础：工作频率



蓝牙设备能够测量接收信号强度（RSS），并相应地通知其配对设备以增加或减少传输功率。这项技术在小型移动设备中特别有用，可以节省有限的电量并延长电池寿命。蓝牙设备的通信范围可以根据电源管理类型的不同而变化，从1米到91米不等。尽管蓝牙设备可以调整其传输功率，但不同设备的功率水平有显著差异。例如，1类设备（如交流电供电的蓝牙设备）的功率为100mW，通信范围可达91米，而2类电池供电设备的功率为2.5mW，通信范围最多为9米。低功耗的3类设备（如蓝牙适配器）在1mW功率水平下只能与1米范围内的邻近设备通信。尽管功率控制不被视为一种安全机制，但它有助于减少被攻击的机会，因为攻击者需要在通信范围内才能发起攻击。



蓝牙版本	数据传输速率
1.1 & 1.2	1Mbps
2.0+EDR & 2.1+EDR	3Mbps
3.0+HS & 4.0	24Mbps

蓝牙设备的数据传输速率取决于其支持的蓝牙标准版本。对于蓝牙1.1和1.2，传输速率最高可达1 Mbps；对于2.0 + 增强数据速率（EDR）和2.1 + EDR版本，传输速率最高可达3 Mbps。通常，吞吐量约为相应数据速率的70%。蓝牙3.0 + 高速（HS）和4.0都支持“基于Wi-Fi的蓝牙”，传输速率可达24 Mbps。然而，在这种情况下，实际的吞吐量取决于载体Wi-Fi网络的性能。

INTRO.

PART.1 发展历程与技术基础

HISTORY & TECH BASIS

ATTACK.

PART.4 安全攻击与防御措施

ATTACK & DEFENSE

APPLY.

PART.2 组网结构

NETWORK STRUCTURE

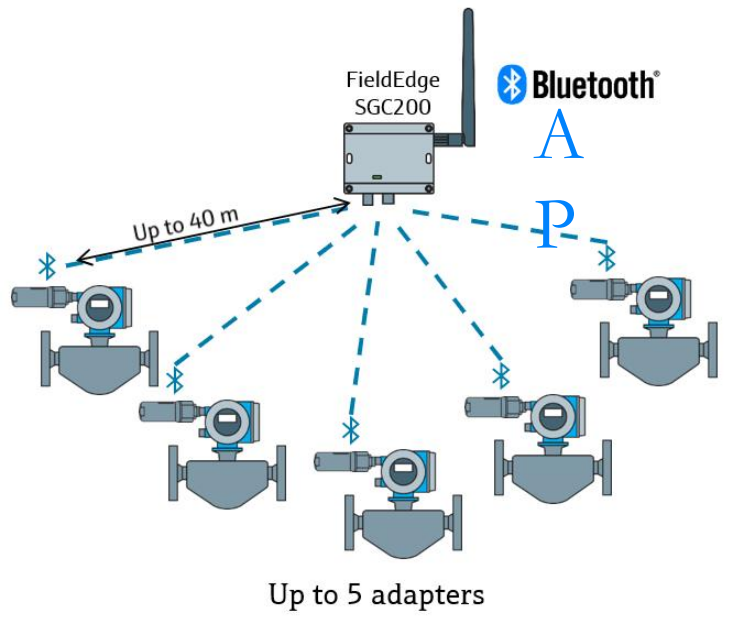
SECURITY.

PART.3 安全目标与四种安全模式

SECURITY GOAL & SECURITY MODES

蓝牙允许两种类型的网络：Ad Hoc网络和基础设施网络。在基础设施网络中，蓝牙接入点（AP）促进了连接蓝牙设备之间的通信，而在Ad Hoc网络中，蓝牙设备无需任何中介即可建立直接连接。Ad Hoc类型的网络比基础设施网络更为常见。

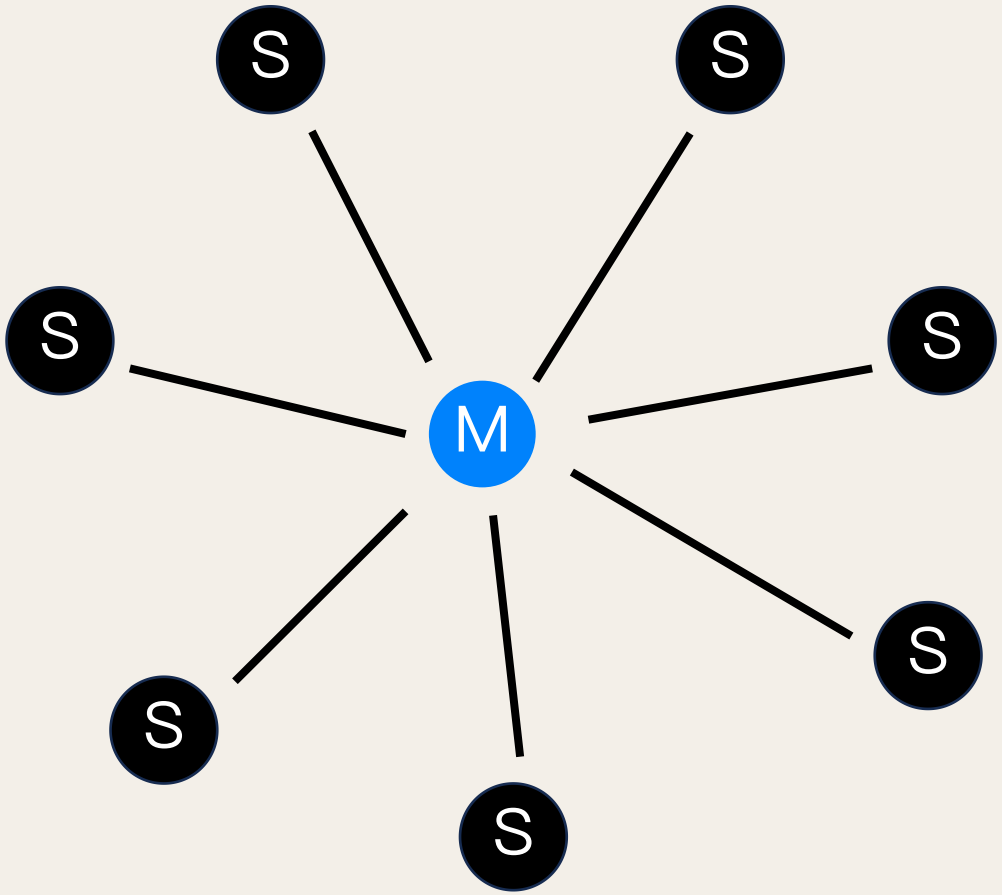
基础设施网络



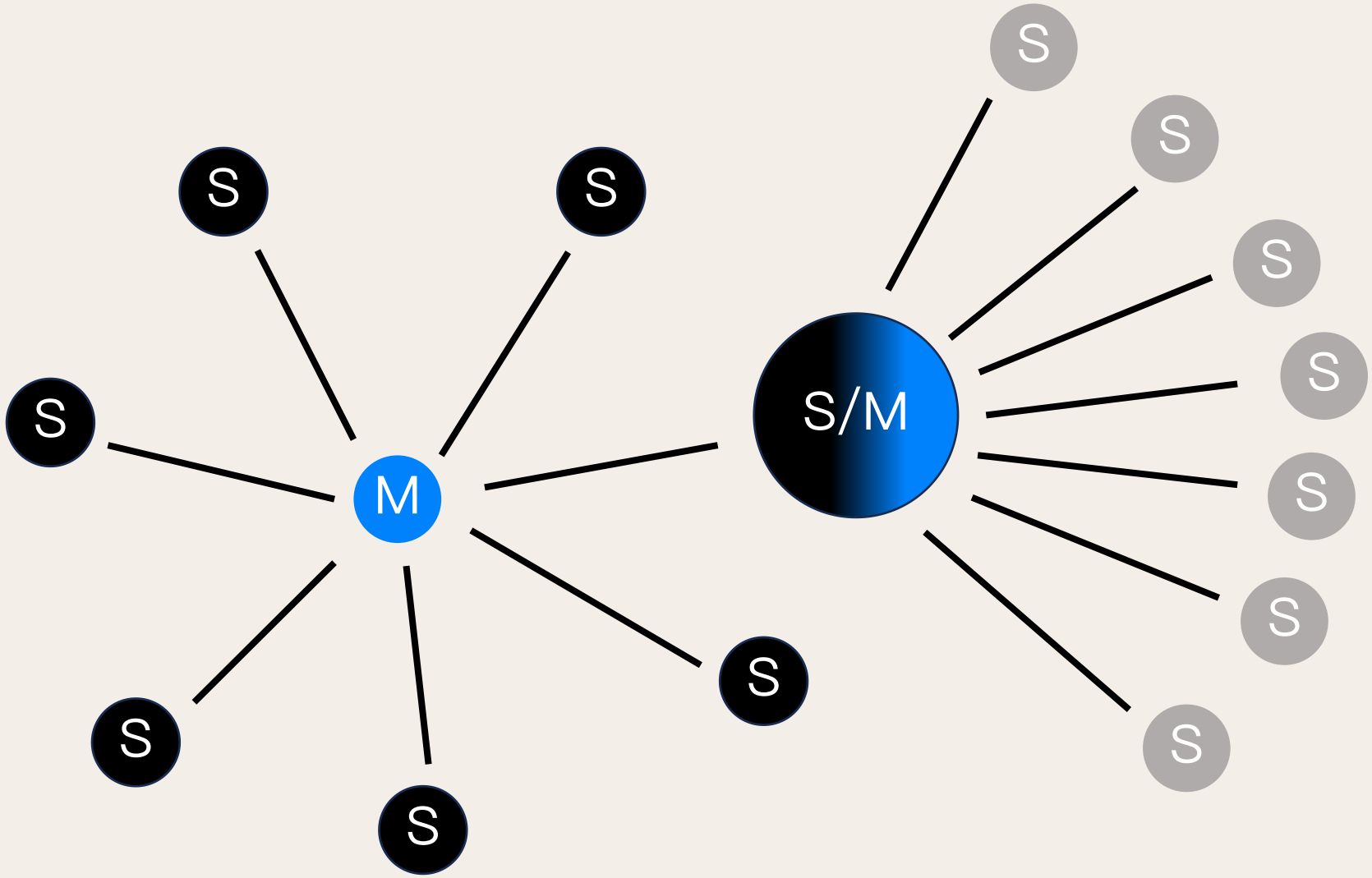
Ad Hoc网络

Ad Hoc网络

一个微微网（piconet, a form of ad hoc）是由最多八个活跃的蓝牙设备组成的集合。其中一个设备被指定为“主”设备，剩下的七个设备为“从”设备。加入微微网后，从设备会与主设备进行时钟同步。主设备与从设备之间的通信可以是一对一或一对多。换句话说，主设备可以与单个从设备、一部分从设备或所有从设备进行通信。



Ad Hoc网络-级联



微微网中的主设备使用时分双工-时分多址（TDD-TDMA）进行通信。TDD-TDMA是一种半双工通信方式，其中主设备使用偶数跳频，而从设备使用奇数跳频。在一对一通信中，主设备均匀地分配通信时间。在一对多通信中，主设备占用50%的信道时间，而从设备以轮流的方式共享剩余的50%信道时间。一个设备可以在当前时隙作为一个微微网的主设备，在下一个时隙作为另一个微微网的从设备。跳频扩展频谱（FHSS）允许从设备转换为主设备后，通过使用不同的跳频序列与其微微网通信，而不会干扰原始微微网。虽然散射（scatternets）是可能的，但由于蓝牙和MAC层规格的限制，实际实现的情况很少。

INTRO.

PART.1 发展历程与技术基础

HISTORY & TECH BASIS

ATTACK.

PART.4 安全攻击与防御措施

ATTACK & DEFENSE

APPLY.

PART.2 组网结构

NETWORK STRUCTURE

SECURITY.

PART.3 安全目标与四种安全模式

SECURITY GOAL & SECURITY MODES

04. 信任级别
服务级别
权限授予

01. 安全目标

PART.3
安全目标
四种安全模式

03. 密钥生成与管理
身份验证
机密性保证

02. 四种安全模式

01.安全目标

蓝牙安全的目标是提供数据机密性、设备认证和授权。
数据机密性是指防止未经授权查看机密数据。
认证涉及验证参与通信的蓝牙设备的身份。与其他类型的网络不同，蓝牙本身并不关注用户认证，例如，任何拥有蓝牙功能智能手机访问权限的人都可以使用配对的车载蓝牙接收器。
授权是在成功认证之后进行的，其目的是确保设备被授权使用某些服务。
接下来的部分将阐述由这些安全目标的衍生出的4种安全模式。

02.四种安全模式

- 安全模式1不提供任何形式的安全性，仅在2.0 + EDR及更早版本中支持。模式1也称为开放模式，在这种模式下，设备不使用任何安全机制，也不会阻止其他设备建立连接。因此，无法验证配对设备的身份，数据也不加密。

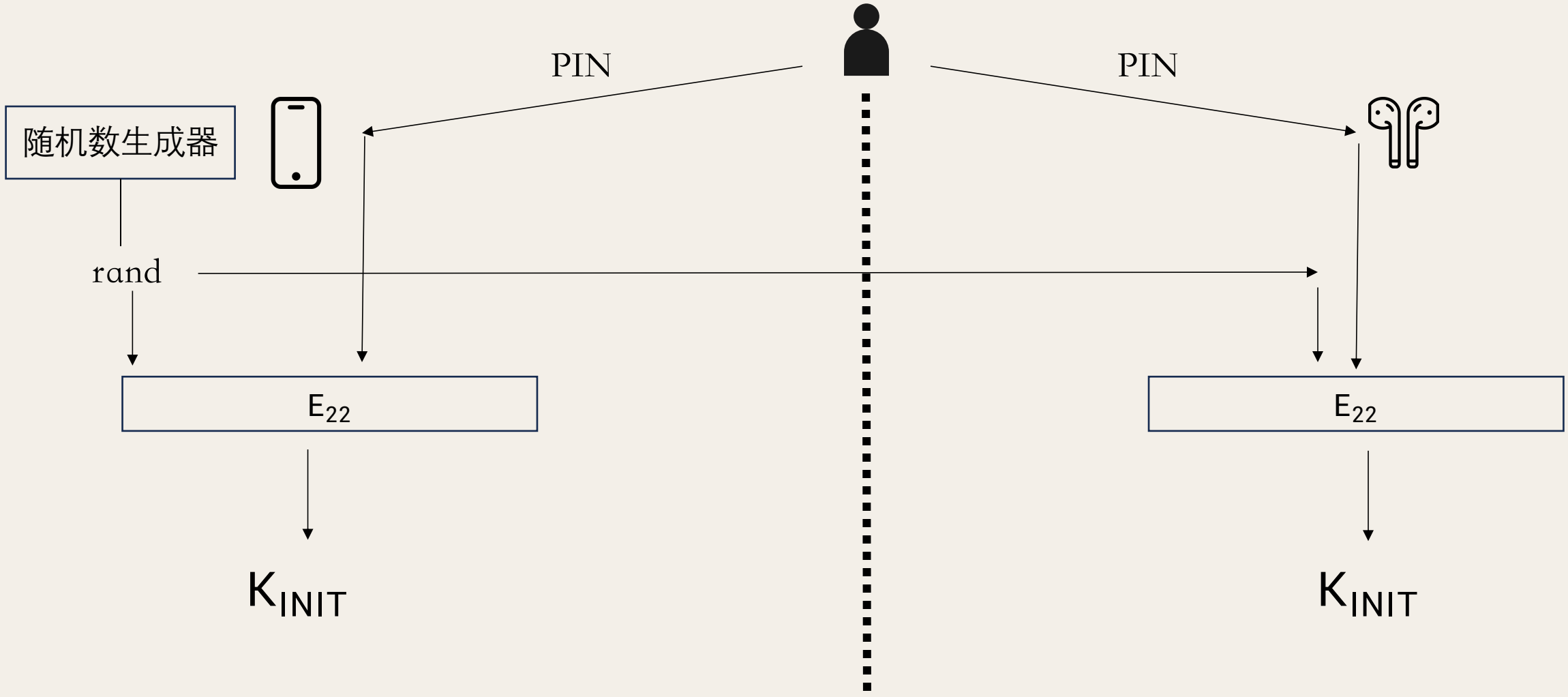
- 安全模式2是一种服务级别强制的安全模式，认证和加密在LMP层实现，其过程在LMP链路建立和L2CAP通道建立之间启动。所有蓝牙设备都支持安全模式2，安全管理器可以决定是否应授予对特定设备的访问权限。为此，安全管理器维护访问控制策略，并与其他协议和设备用户进行接口通信。为了满足同时运行的不同应用程序的安全需求，需要定义多种安全策略和信任级别以限制访问。例如，在安全模式2中，设备A可能有权访问设备B，但同时被阻止访问设备C。

- 安全模式3，支持v2.0 + EDR设备，是一种链路级别强制安全模式，这意味着在物理链路完全建立之前就启动安全程序。所有连接的双向认证和加密（使用对称密钥加密）都是强制性的。

- 安全模式4与安全模式2类似，也是一种服务级别强制安全模式，其中安全程序在链路建立后启动。虽然认证和加密算法保持不变，但在安全配对过程中使用椭圆曲线Diffie-Hellman (ECDH)算法进行链路密钥生成和密钥交换。在这种模式下，安全需求分为链路密钥需要经过认证、链路密钥无需认证或不需要任何安全性。通信中使用的安全简单配对模型将决定模式4应用上述哪种安全需求。

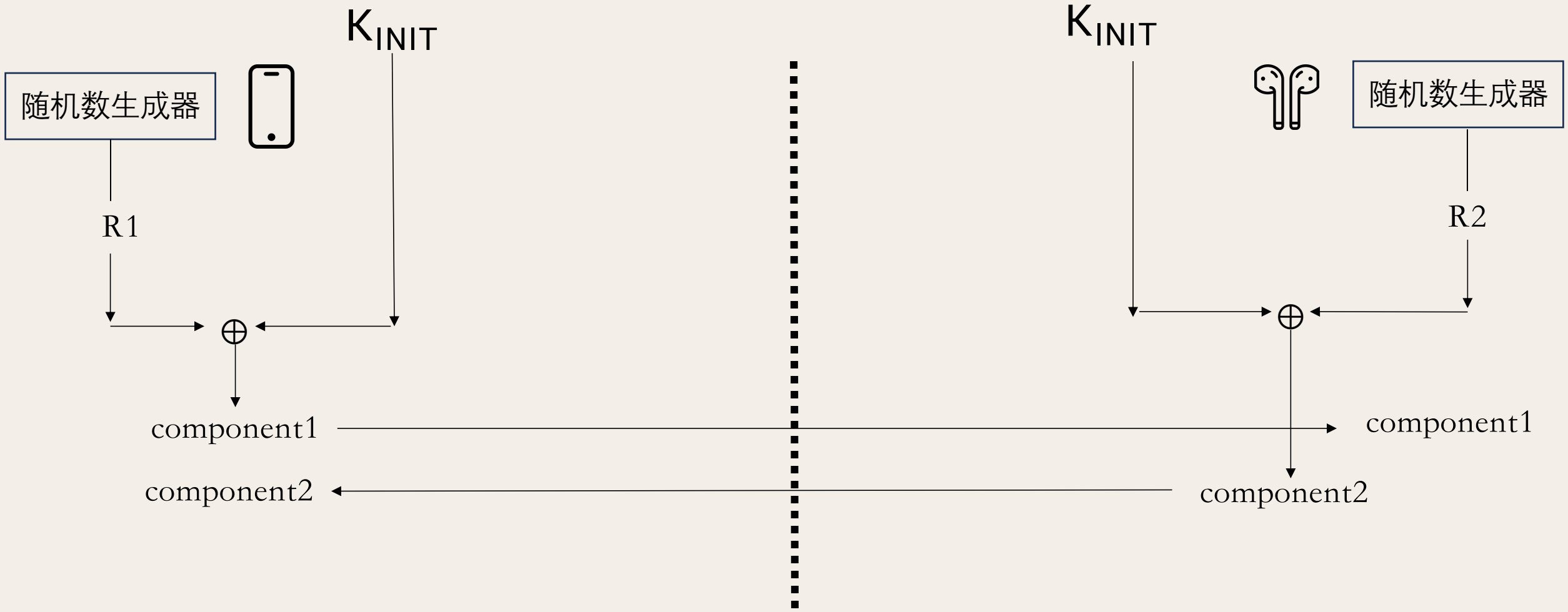
03. 密钥生成与管理

在安全模式 2 和 3 中，生成链接密钥的方法是相同的，但与安全模式 4 中使用的链接密钥生成方法不同。



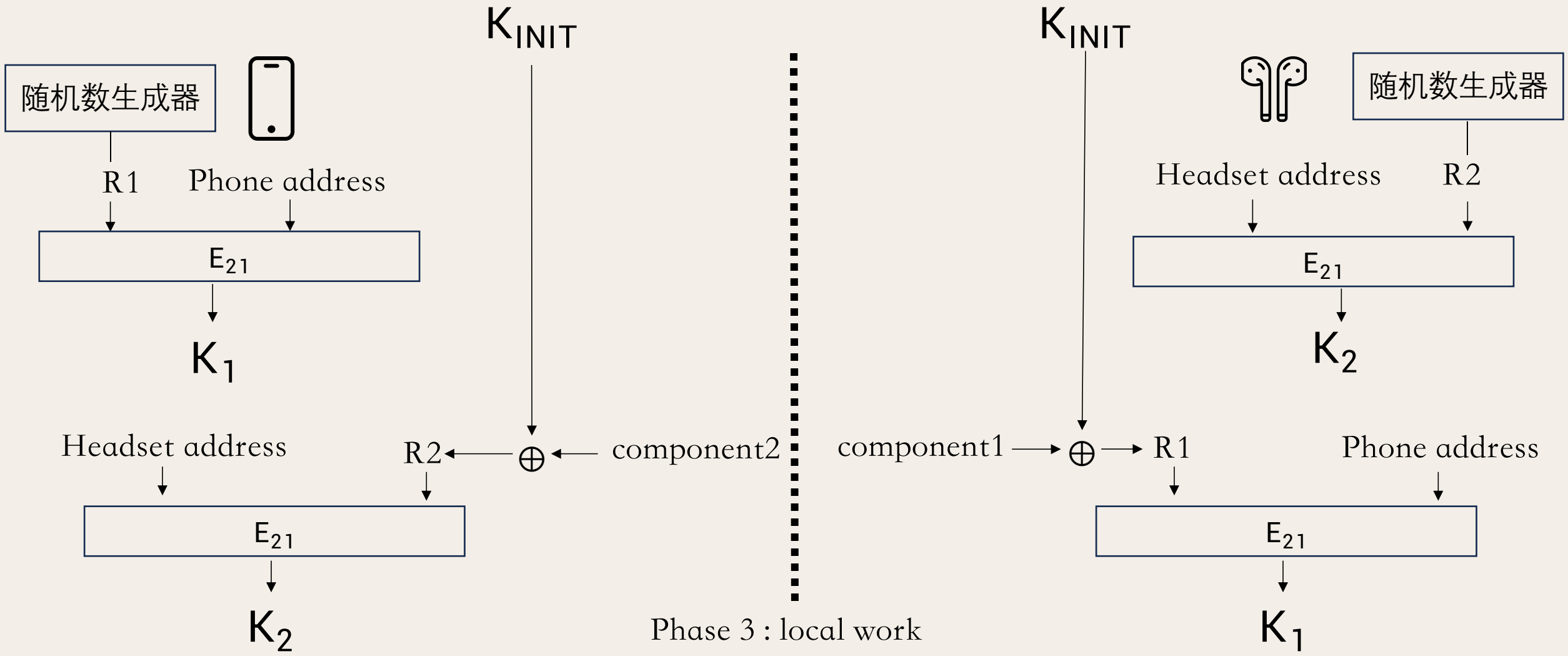
Phase 1 : init sync

03. 密钥生成与管理

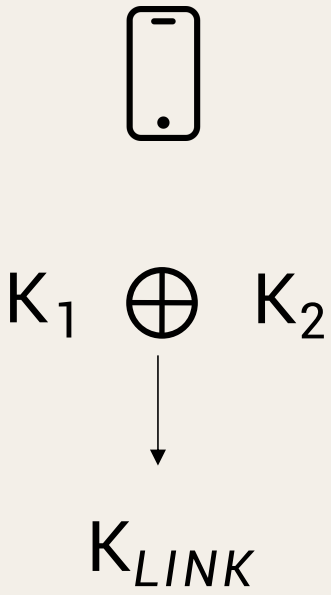


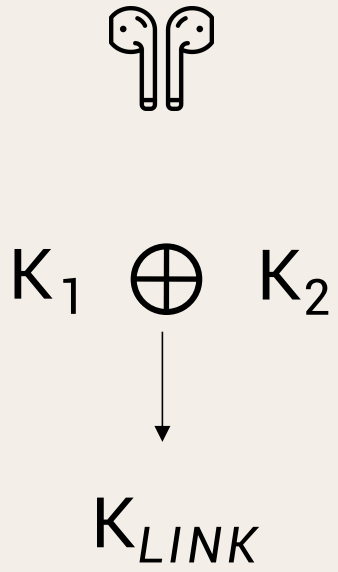
Phase 2 : component

03. 密钥生成与管理


K_{INIT}
随机数生成器
R1
Phone address
E_{21}
K_1
Headset address
R2
component2
E_{21}
K_2
Phase 3 : local work
K_{INIT}
随机数生成器
Headset address
R2
E_{21}
K_2
component1
R1
Phone address
E_{21}
K_1

03. 密钥生成与管理





Phase 4 : key sync

03. 密钥生成与管理：安全模式4密钥生成

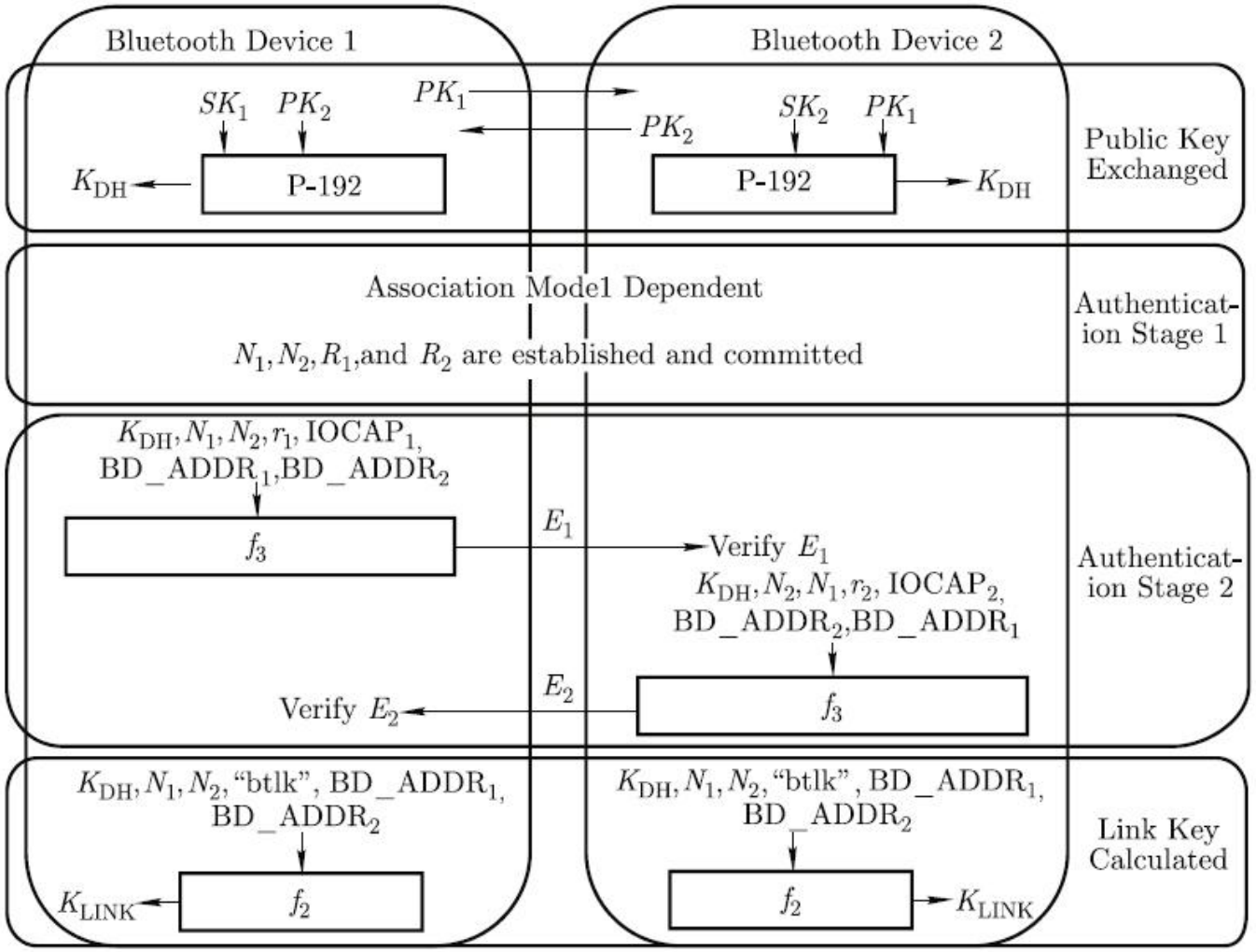


Fig. 5.2 Bluetooth link key establishment for secure simple pairing in security Mode 4.

步骤 1 设备发现：在此步骤中，SAP 客户端寻找支持 SAP 服务器的设备。需要的蓝牙设备地址可以通过蓝牙查询获得。扩展查询响应标签可以帮助过滤 SAP 服务器设备，因此用户可以轻松识别已知的 SAP 服务器。

步骤 2 连接建立：SAP 服务器在启动 L2CAP 信道建立之前启动身份验证。

步骤 3 IO 能力和公钥交换：为了确定在配对中应使用哪种配对模型，需要交换 SAP 客户端和服务器的 IO 能力。双方还交换椭圆曲线 Diffie-Hellman 公钥。在此步骤结束时，两台设备都会派生出 KDH。

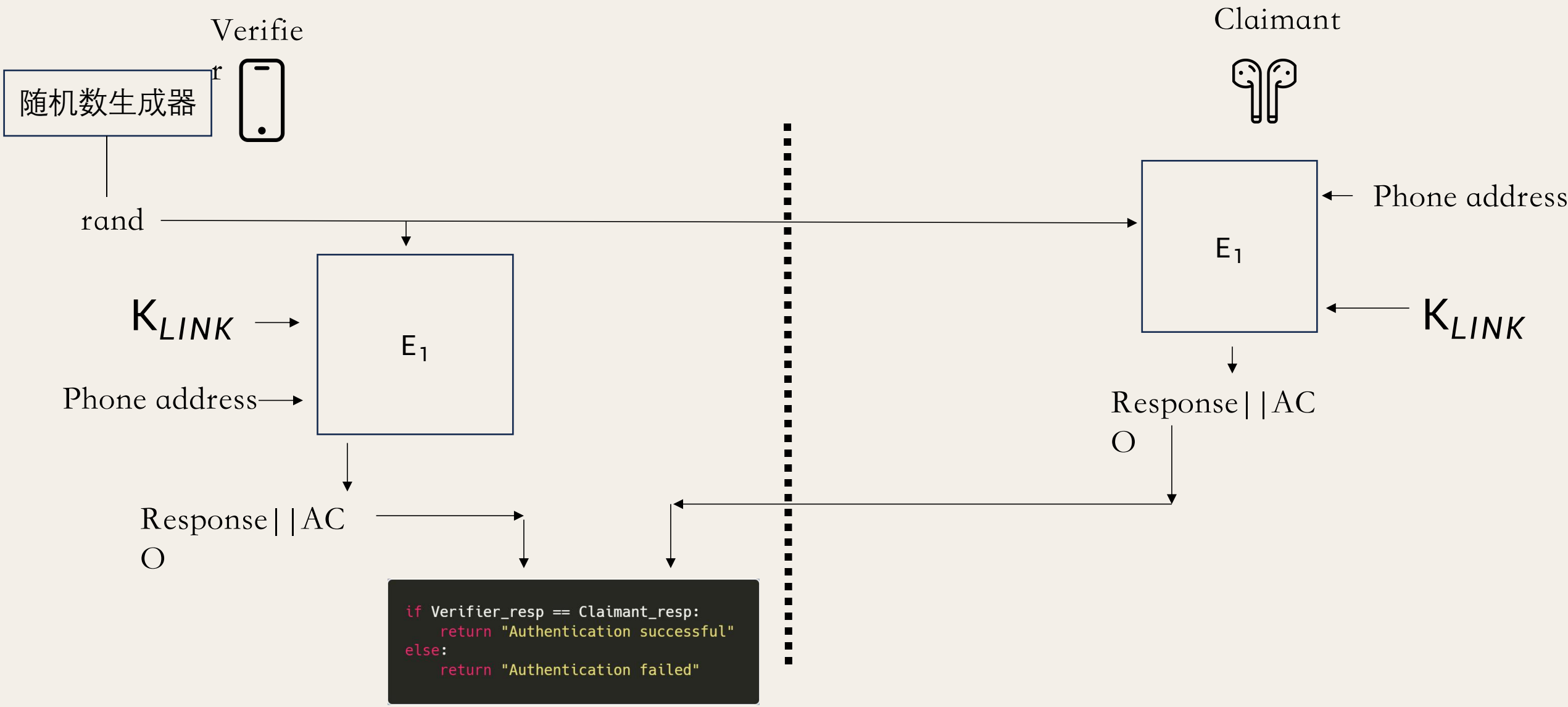
步骤 4 认证阶段 1：第一阶段根据所使用的配对模型略有不同。无论配对模型如何，此认证阶段的目的是在设备上显示一个六位数字，并让用户在配对设备上输入相同的数字。

步骤 5 认证阶段 2：在此阶段，SAP 客户端和服务器上比较加密函数的结果，如果匹配，双方将继续计算链接密钥。

步骤 6 链接密钥计算：生成链接密钥 KLINK，并进行相互认证以确保 KLINK 确实由双方共享。

步骤 7 启用加密：一旦链接密钥建立，SAP 客户端开始 L2CAP 信道建立过程。密钥生成和交换过程结束。

03. 密钥生成与管理：身份认证




```
if Verifier_resp == Claimant_resp:
    return "Authentication successful"
else:
    return "Authentication failed"
```

03. 密钥生成与管理：机密性

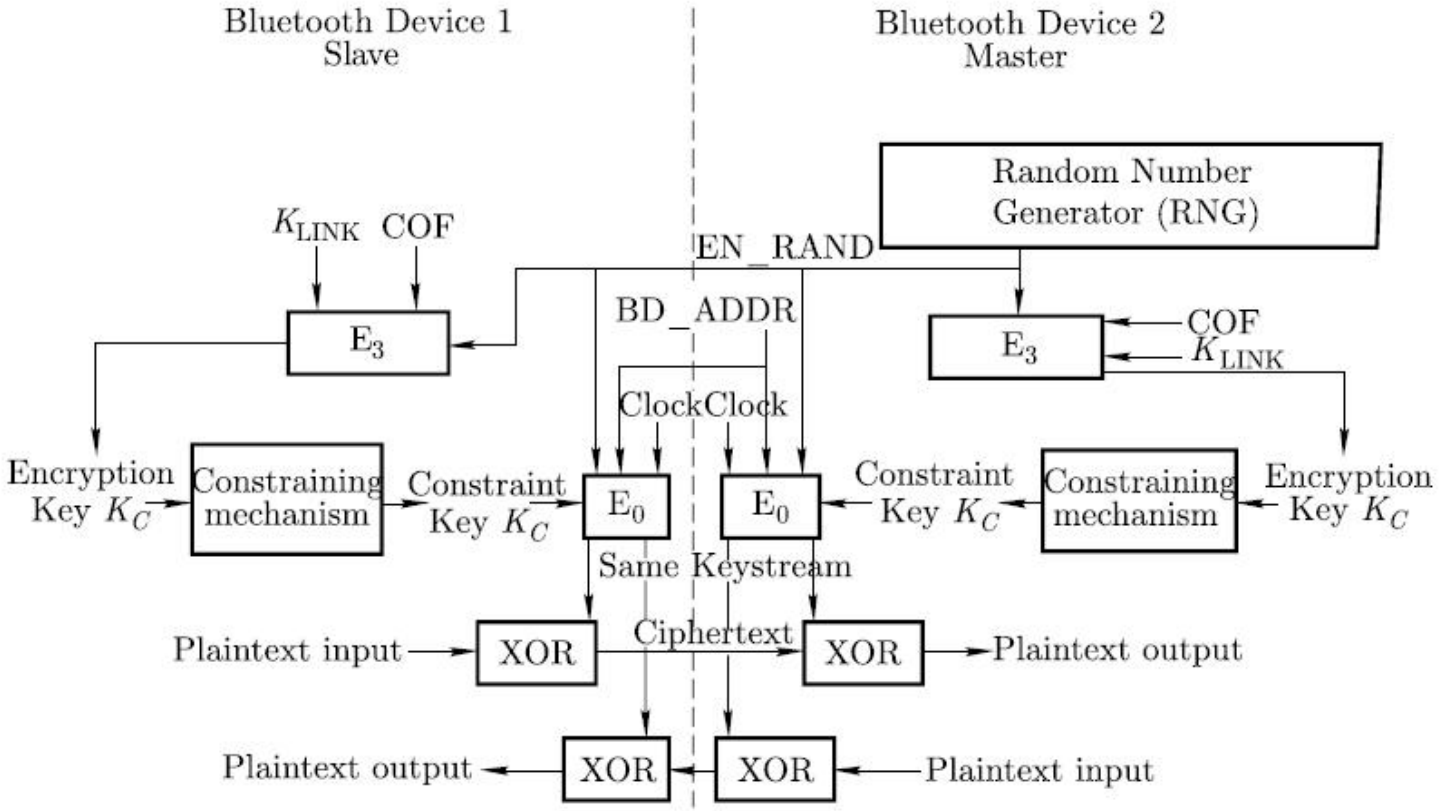


Fig. 5.4 Bluetooth Keystream generation and encryption procedure.

蓝牙不仅提供了前面讨论的安全模式，还提供了一个单独的机密服务，以增强数据机密性。在三种加密模式中，模式 1 不需要加密，模式 2 只需要使用各自链接密钥对单独地址流量进行加密，而模式 3 强制对所有流量使用基于主链接密钥的加密密钥进行加密。

如图 5.4 所示，上半部分的操作在从设备和主设备上生成相同的密钥流。双向加密仅是将生成的密钥流与明文进行异或运算，而解密是将相同的密钥流与密文进行异或运算。为了生成密钥流，双方使用 E0 算法，并使用以下输入：随机数 EN RAND、主设备的地址 BD ADDR、时钟和约束加密密钥 KC。KC 是使用 E3 算法，以链接密钥、EN RAND 和 COF 为输入派生出来的。

04.信任级别、服务级别、权限授予

除了安全模式外，蓝牙还提供两个信任级别和三种不同的安全服务级别，每个不同的安全需求，例如认证、授权和加密，都可以独立配置

信任等级	设备间关系及获取服务的权限
信任	确定性关系，拥有全部权限
不信任	无关系，仅有部分访问权限

服务级别	认证	授权	访问
级别 1	必需	必需	仅自动授予受信设备访问权限
级别 2	必需	不需要	仅在成功认证后授予访问权限
级别 3	不需要	不需要	自动授予访问权限

INTRO.

PART.1 发展历程与技术基础

HISTORY & TECH BASIS

ATTACK.

PART.4 安全攻击与防御措施

ATTACK & DEFENSE

APPLY.

PART.2 组网结构

NETWORK STRUCTURE

SECURITY.

PART.3 安全目标与四种安全模式

SECURITY GOAL & SECURITY MODES

- 蓝牙劫持：这种攻击利用了旧设备固件中的一个漏洞。通过强制连接到设备，此类攻击可以访问存储的数据和国际移动设备识别码（IMEI），这可能导致将来电重定向到攻击者的设备。推荐的对策是首先更新蓝牙设备，使用最新的操作系统和软件。如果硬件是通用的且不支持当前的安全标准，则考虑更新硬件。此外，在蓝牙设备未主动交换数据时，将其保持在不可发现模式也很重要。
- 蓝牙诱骗：类似于电子邮件垃圾信息和网络钓鱼，蓝牙诱骗攻击会向启用蓝牙的设备发送未经请求的消息，诱使用户进行某些活动，例如在联系人列表中添加信息。防御对策包括在某些公共区域（如购物中心）不使用时关闭蓝牙设备，并从菜单中将设备设置为隐藏、不可见或不可发现模式。
- 蓝牙窃听：在这种攻击中，可以通过利用旧设备固件中的漏洞来访问设备和命令。用户通常不知道这种攻击的存在，攻击者可能会访问数据、通话和其他服务。对策包括更新蓝牙设备的硬件和软件，并要求进行身份验证。
- 拒绝服务攻击 (DoS)：类似于其他类型的无线通信中的 DoS 攻击，此类攻击通过发送大量消息来压垮目标设备，使其冻结或耗尽电池。由于通信范围短，用户在检测到此类攻击时可以简单地将设备带出危险区。防御 DoS 攻击的最佳方法是通过关闭设备或将其隐藏在不可发现模式来限制设备的可发现性和连接性。

Thanks