第一部分是背景介绍

1.**AKE**是验证性密钥交换,指在密钥交换协议中交换会话密钥，同时验证参与密钥交换的各方的身份。

它是一个端到端的非对称认证协议。由AKE衍生出许多的扩展，如：PAKE（password-ake）连接到个人wifi使用的就是PAKE

传统AKE的弊端：

（1）由于密钥通常存储在终端中，密匙及其容易被窃取。

（2）消息传递应用程序不能立即确定密钥是否被克隆。

（3）当参与者丢失或更换终端时，很难及时更新公钥-秘密密钥对，因为每个新的公钥在启用之前都需要通过带外方式进行认证。

2.**关于消息传递：**社交消息应用以其便捷性成为日常交流的主流手段，这个图示2022年一月份全球最流行社交app排名，从中可以看出 whats app高居第一，几乎所有的社交App都是端到端通讯的，**其中whatsApp、FaceBook是端到端加密，而微信、qq不能进行端到端加密** 因为根据《中华人民共和国反恐怖主义法》第18条及第19条规定通讯软件是不可以进行端到端机加密的。所以这些加密技术在社交app上只能用在国外这些app上。

我们看WhtasAPP关于其端到端加密技术的描述可以很显然的看出采用的是传统的公钥技术。

其中对于每一个会话都会生成一对特殊密匙，外部显示为安全代码。

4.关于几种生物特征的指标：我们可以看出其中指纹与虹膜的综合指标都是很好的，本文采用指纹**和**虹膜，前者容易采集成本低同时效率很高，后者成本稍高但是防伪、稳定性，特征多样性都极其之高。

第二部分我们开始正式介绍BAKE

所谓BAKE就是要 参与者根据自身的生物特征生成秘钥和相应的公钥，最后经过BAKE协议生成会话密匙。它的优点是：（1）会话密钥是为经过身份验证的用户协商的，而不是经过身份验证的随机公钥。（2）无需存储在终端中，并且在更换终端时不需要更新密钥和相应的公钥。

它也有非常明显的缺点：生物特征是永久性的，这意味着密钥泄露后无法更新。 但幸运的是：。。。。

为了保证是**从随机字符串中导出一个会话密钥，这些字符串只有具有正确生物特征的参与者才能访问。**
AFEM：非对称模糊封装技术将消息封装为一个公共的与目标密钥相对应的密钥。 只有参与者谁拥有与目标密钥接近的密钥，就可以获得来自封装消息的随机字符串。

AFEM由这样一个四个函数组成：

Setup： 它生成一组公共参数，这是对以下算法的隐式输入。

PubGen：该公钥生成算法以密钥∈SK作为输入。 它输出一个公钥。

Enc: 该封装算法以公钥和普通消息∈S作为输入。 它输出封装的消息。

Dec: 该确定性解封装算法以密钥∈SK和封装后的消息作为输入。它输出解封的消息。

接下来我们具体介绍BAKE的过程：如果所示，BAKE有三个阶段：

（1）初始化（init）：两个参与者同意一组公共参数来初始化整个系统。

（2）密钥生成（KeyGen）：每个参与者基于他们的生物特征生成公钥，并将公钥发送给另一个参与者。

（3）AKE（认证密匙交互）：发送方向接收方请求彼此认证并协商可用于建立安全信道的会话密钥，参与者需要她/他的生物特征和其他参与者的公钥作为该阶段的输入。

如右图所示，是具体使用AFEM四个函数的BAKE框架的具体细节。

基于细节点的指纹向量集生成算法的具体细节就是：

个细节点都被初始化为中心点，然后，选择直线最近的μ个点根据算法生成向量集，如这个例子设置μ为4，Point i就是点i，point i，j就是离i第j近的点。

评价

更进一步的比较 将Bake与 Fuzzy aPAE进行在生物特征向量和生物特征向量集上的的运行时间和计算消耗进行对比，可以看出Bake是具有明显优势的。

问题：

1. 该方案在实际生活中的实用性怎么样？

   我觉得这篇文章中提出的Bake框架还有其中对于生物特征的转化、AFEM的提出、噪声避免算法的设计是由研究意义的。在实际生活中，设计更多的生物特征算法，让用户自己选择采用哪种来加密数据。总的来说，我觉得实用性是有的。

2. 我听你说这篇论文采用的是基于细节点的指纹识别技术，为什么不采用别的识别技术呢？

   如果采用别的技术，例如指纹编码，因为图像旋转提取出来的指纹向量应用在AFEM上得到的密钥会不同。而这个基于细节点的识别技术是采用的相对位置，所以更适合AFEM机制。

3.