# Gait-Key: A Gait-Based Shared Secret Key Generation Protocol for Wearable Devices

Authors:
WEITAO XU; CHITRA JAVALI; GIRISH REVADIGAR;
CHENGWEN LUO; NEIL BERGMANN; WEN HU;

Publication: ACM Transactions on Sensor Networks January 2017

唐慧敏
51205902133

# 背景

近年来，智能可穿戴设备的数量出现了显著增长。对于这些可穿戴设备，一个重要的安全问题是在合法设备之间建立一个经过身份验证的通信通道，以保护后续的通信。由于无线通信和资源的限制，提供安全、高效和用户友好的设备配对是一项具有挑战性的任务。

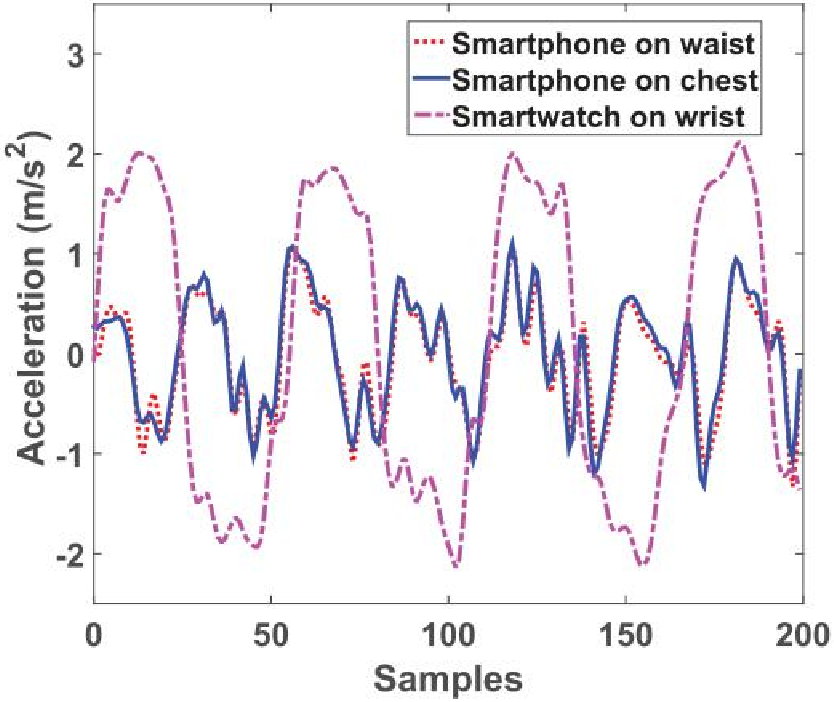
**传统解决方案:**

- **显示输入**
- **点对点密钥交换算法**

**本文提出的解决方案:**

**Gait Key —— 基于步态的共享密钥生成方案**

# 挑战



两个挑战：

•步态产生的信号被手臂摆动产生的噪声信号干扰

•可穿戴设备的计算能力和电池容量受到限制

解决方案：

•盲源分离技术(BSS)

•采用轻量级的信号处理技术、AES、哈希计算

# 流程图

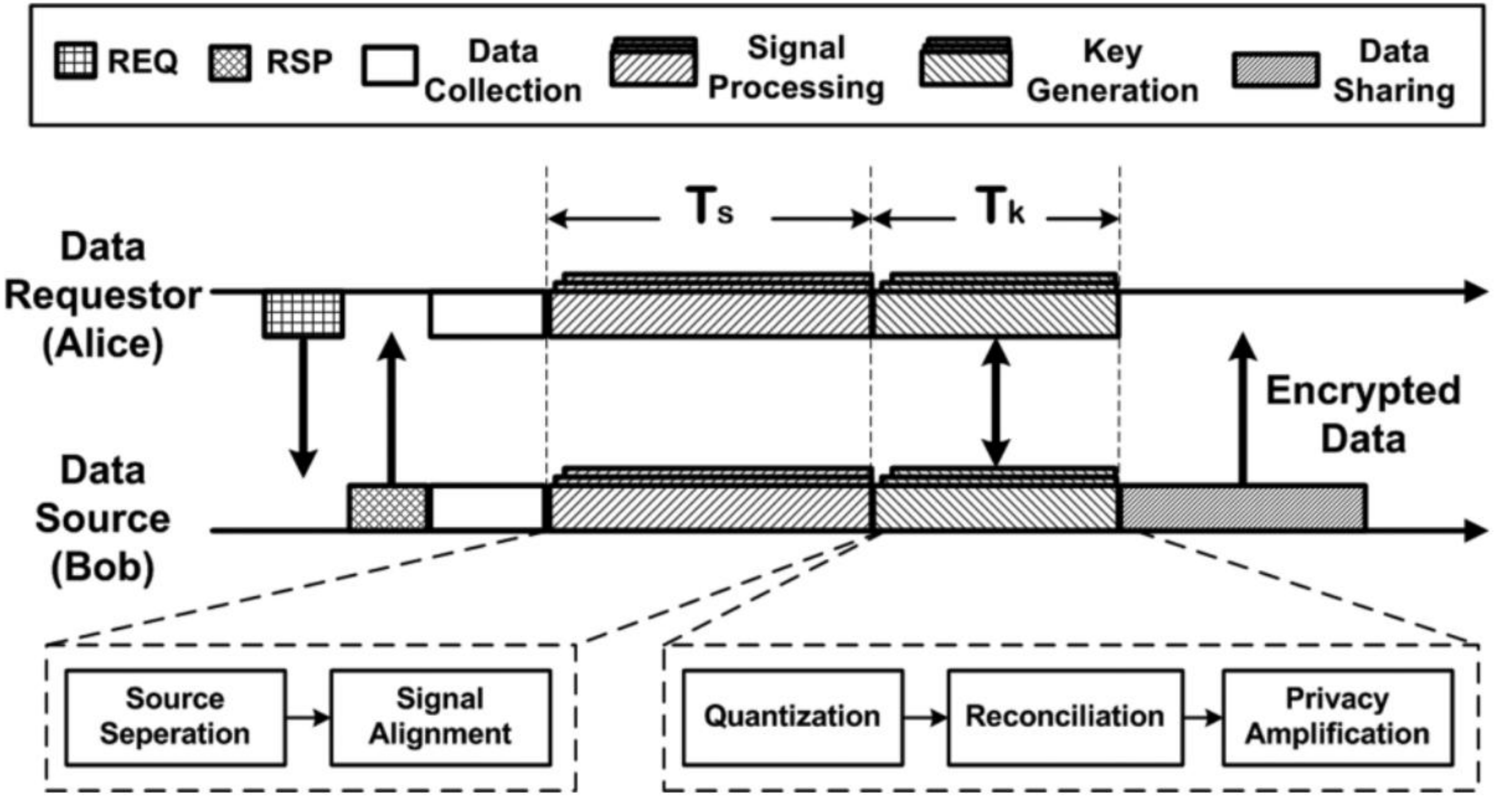


Fig. 3. Flowchart of the key generation scheme.

# 流程图

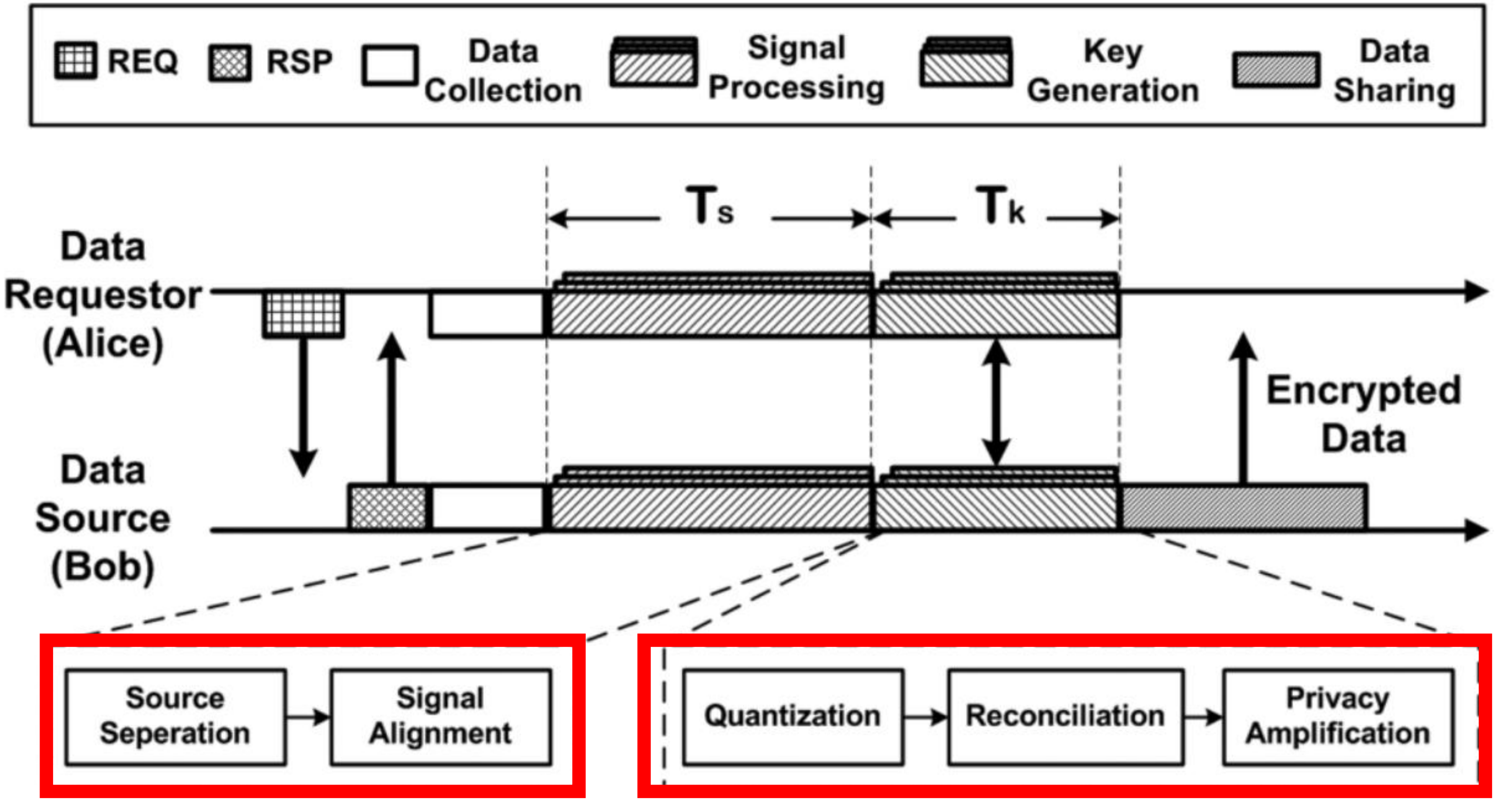


Fig. 3. Flowchart of the key generation scheme.

# 信号处理

## 1. 信号分离——ICA技术

ICA是指在只知道混合信号，而不知道源信号、噪声以及混合机制的情况下，分离或近似地分离出源信号的一种分析过程。

前提：

（1）对于每个位置，我们附加一个三通道的加速度计量器，因此我们有三个通道的观测，信号主要来自于：手臂摆动和行走；

（2）在每个传感器位置，不同来源的加速度线性混合；

（3）身体各部分的运动模式是独立的，而步态是身体各部分结合得到的总体模式；

（4）信号通过身体传输的时间延迟是可以忽略的；

（5）身体运动产生的加速度值的统计分布不是高斯分布；

# 信号处理

假设用户的一只手腕上戴着智能手表，通过内置的三通道加速度计测量的线性加速度为Acc(t)。由于**手腕上记录的加速度计信号分别是腿部和手臂摆动信号的混合**，因此我们问题的ICA模型可以写成

$$Acc(t) = A \cdot S(t), \tag{1}$$

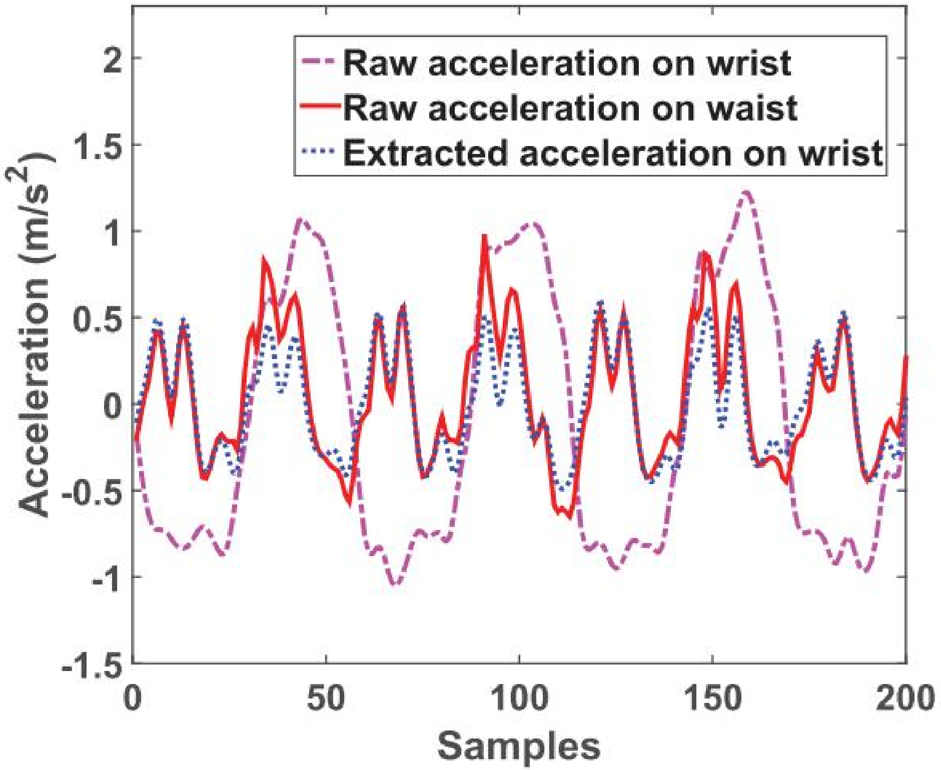
其中A为混合矩阵，S(t)为独立源，我们的目标是找到一个W（A的逆矩阵）,以此来计算源信号：

$$\tilde{S}(t) = W \cdot Acc(t) = W \cdot A \cdot S(t). \tag{2}$$

没有手臂摆动的加速度可以表示为：

$$\mathrm{Acc}'(t) = \mathrm{W}\overline{\mathrm{S}}$$

$$\overline{\mathrm{S}} = \begin{bmatrix} \overline{s}_{11} & \overline{s}_{12} & \dots & \overline{s}_{1n} \\ 0 & 0 & \dots & 0 \\ \overline{s}_{31} & \overline{s}_{32} & \dots & \overline{s}_{3n} \end{bmatrix} \tag{3}$$

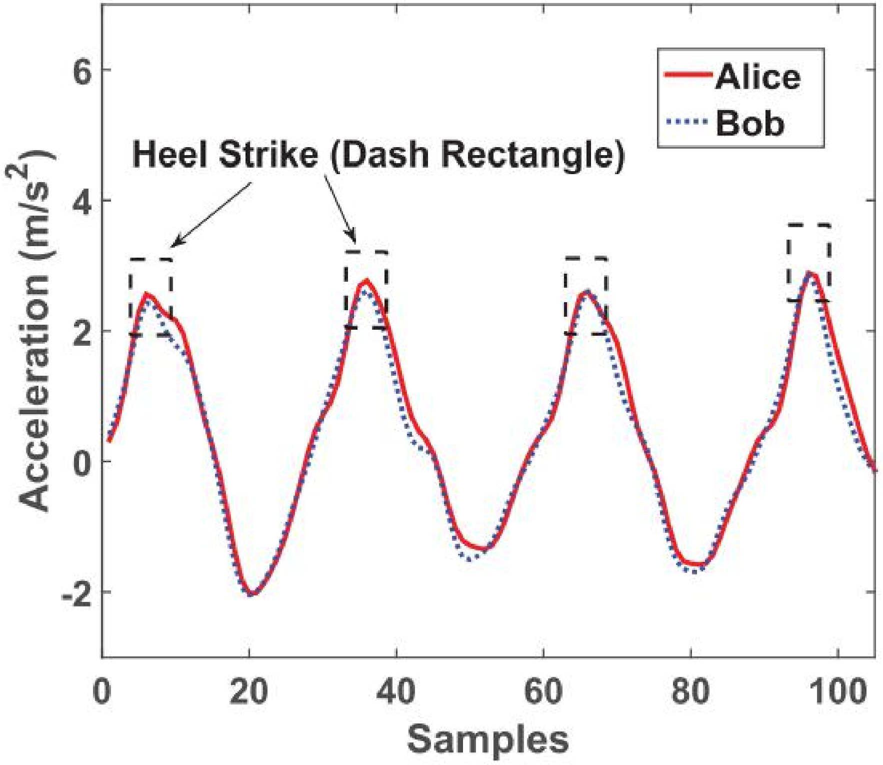


# 信号处理

## 2.信号同步

（1）时间同步

在这项工作中，我们使用了一种基于事件的方法，其中设备检测脚跟撞击（Heel Strike）事件的时间点，使用这个事件作为锚点。在没有通信的情况下，脚跟撞击事件可以在每个设备上本地检测到，这消除了设备之间显式同步的需要。



# 信号处理

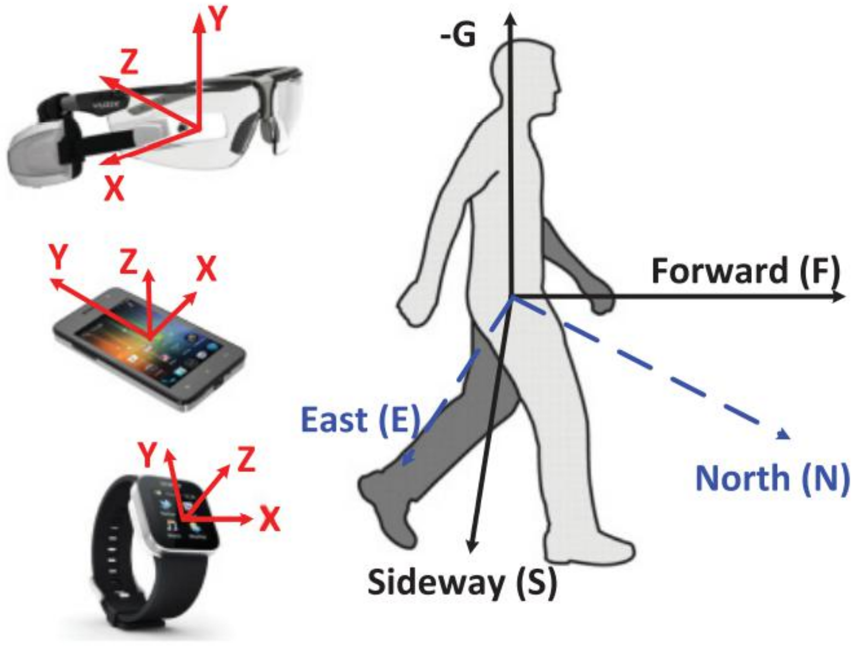
## 2.信号同步

（2）空间同步：引进了一种独立于方位和位置的公共物体参考坐标系。以智能手机为例，假设智能手机沿三个正交方向的线性加速度信号分别为Accx、Accy、Accz。在物体参考系中的线加速度可以计算为：

$$\begin{bmatrix} Acc_G \\ Acc_F \\ Acc_S \end{bmatrix} = R_b^w \cdot R_w^d \cdot \begin{bmatrix} Acc_x \\ Acc_y \\ Acc_z, \end{bmatrix}$$

从世界坐标系到身体坐标系的旋转矩阵

从设备坐标系到世界坐标系的旋转矩阵

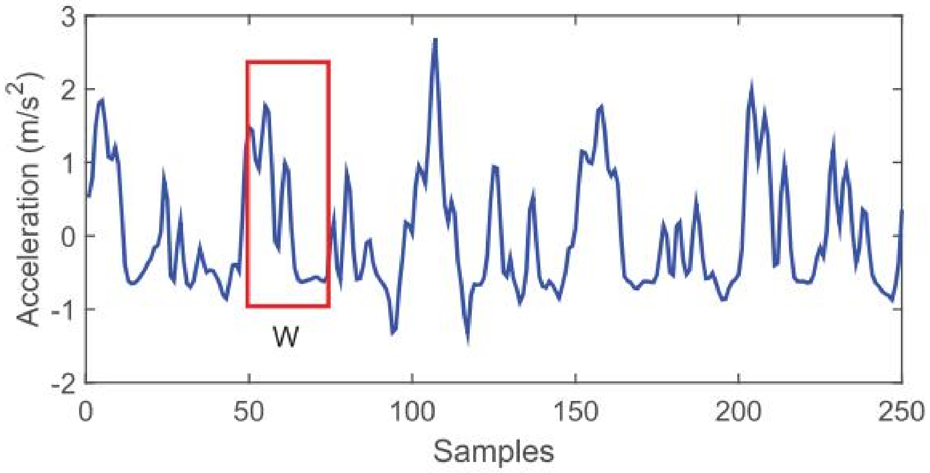


# 密钥生成

## 1.多层量化

We perform filtering, then quantization for the acceleration values along the three directions separately. We first apply a low-pass filter for noise reduction. The cutoff frequency is chosen as 10Hz, as the useful frequency of human motion lies below 10Hz.

More specifically, we segment the acceleration values with a moving window with no overlap (window size W). Thereafter, for each window, we generate bits by the following steps:



# 密钥生成

## 1.多层量化

（1）确定位数的上界

先计算样本的近似熵: $\varepsilon = -\sum_a p(a)\log_2 p(a)$

量化级的上界为: $\mathrm{m}_{\max} \le 2^{\varepsilon}$

（2）确定量化区间

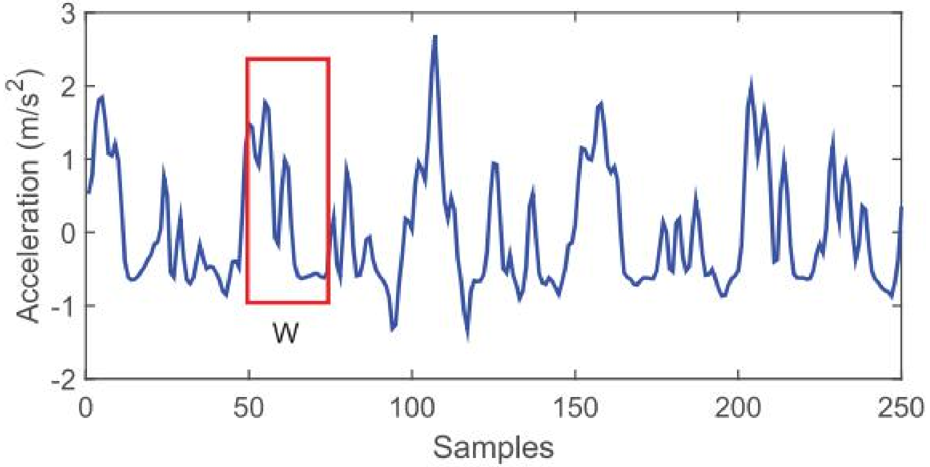
单个量化区间由以下方程表示:

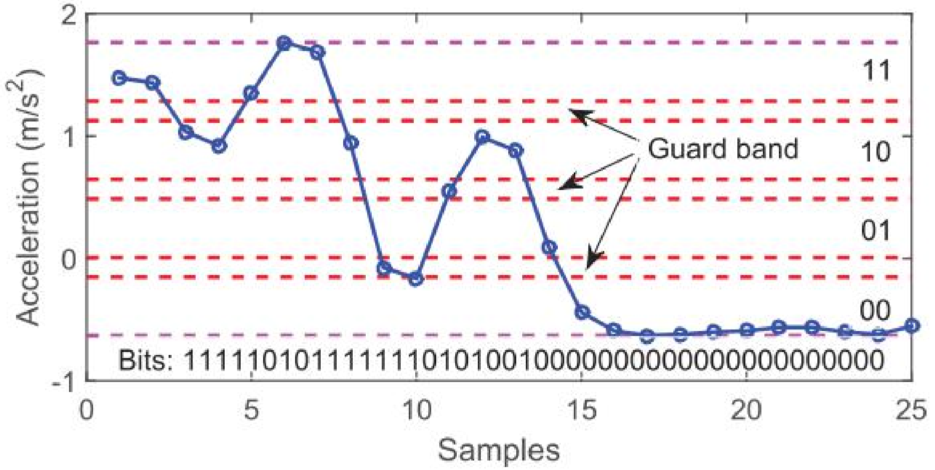
$$I_0 = (q_0, q_1 - g_1], I_1 = (q_1, q_2 - g_2], \ldots, I_{m-1} = (q_{m-1}, q_m]$$

量化区间的长度和保护带的大小由此计算:

$$\int_{q_{i-1}}^{q_i - g_i} f_a da = \frac{1-\alpha}{m}, \int_{q_i - g_i}^{q_i} f_a da = \frac{\alpha}{m-1}$$

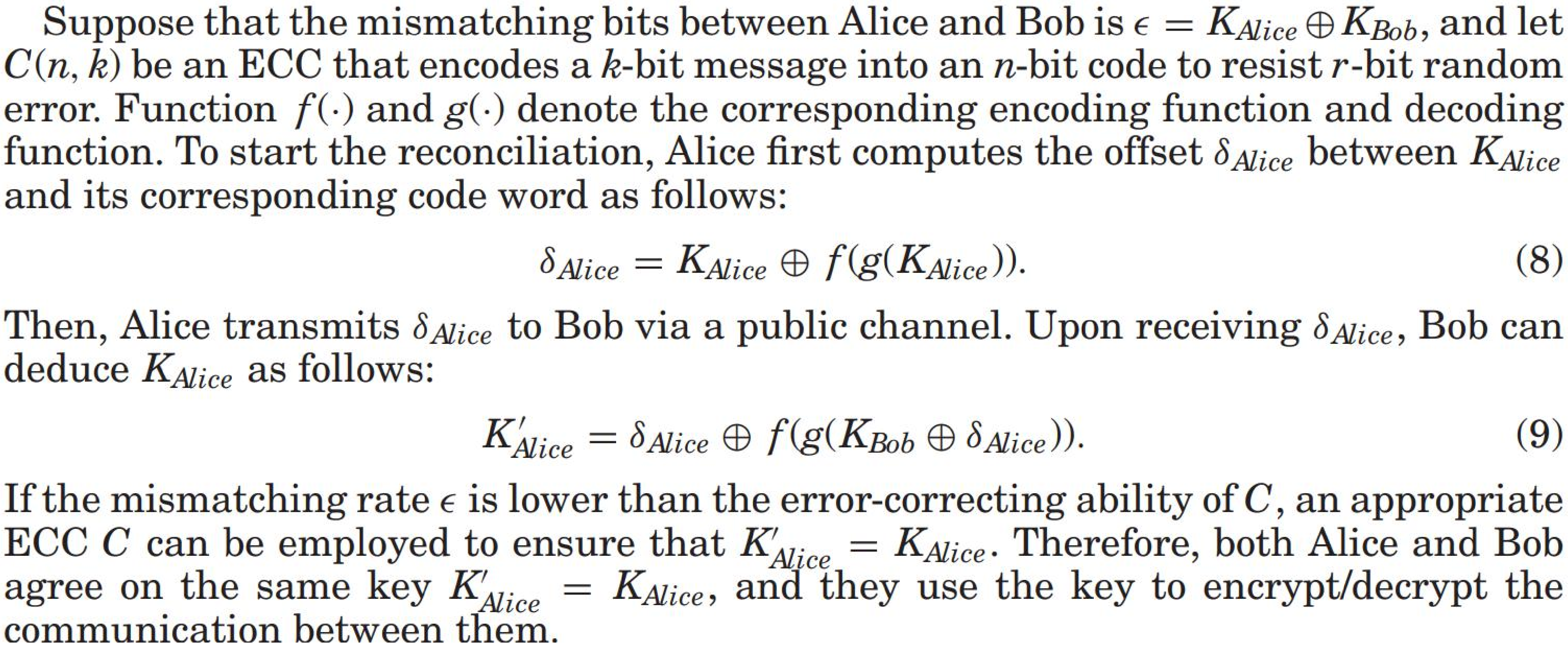
（3）提取密钥: [KG, KF, KS]





# 密钥生成

## 2.解决不匹配问题——ECC纠错码（the error correction code）



Suppose that the mismatching bits between Alice and Bob is $\epsilon = K_{Alice} \oplus K_{Bob}$, and let $C(n, k)$ be an ECC that encodes a $k$-bit message into an $n$-bit code to resist $r$-bit random error. Function $f(\cdot)$ and $g(\cdot)$ denote the corresponding encoding function and decoding function. To start the reconciliation, Alice first computes the offset $\delta_{Alice}$ between $K_{Alice}$ and its corresponding code word as follows:

$$\delta_{Alice} = K_{Alice} \oplus f(g(K_{Alice})). \qquad (8)$$

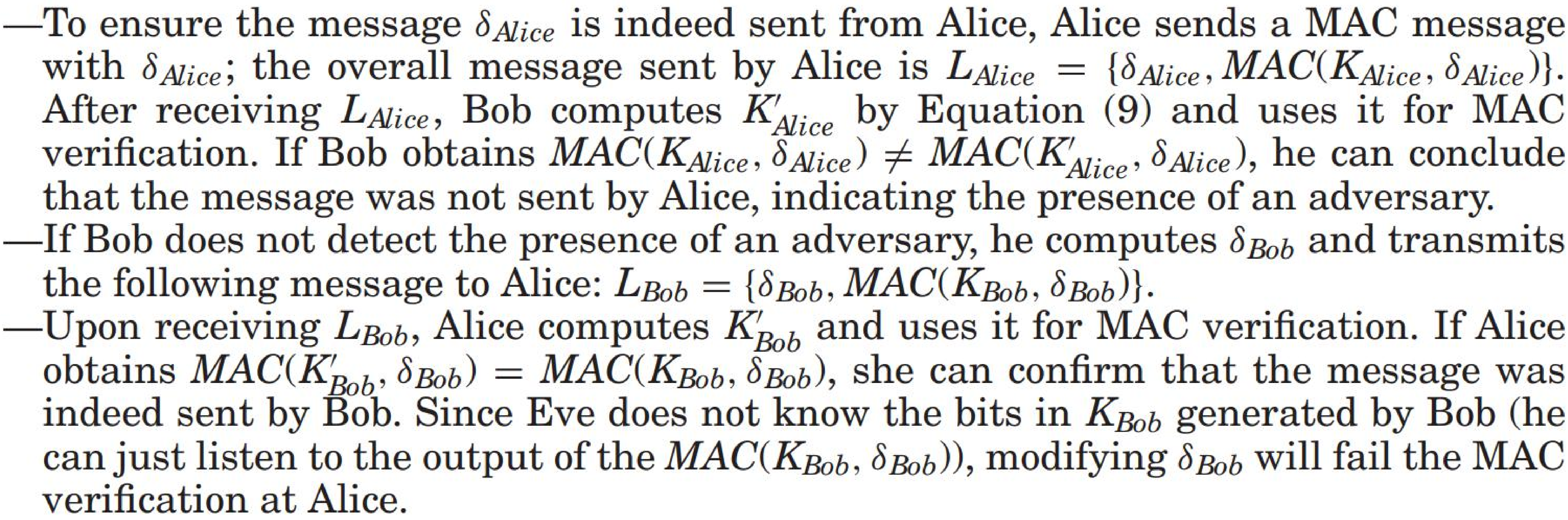
Then, Alice transmits $\delta_{Alice}$ to Bob via a public channel. Upon receiving $\delta_{Alice}$, Bob can deduce $K_{Alice}$ as follows:

$$K'_{Alice} = \delta_{Alice} \oplus f(g(K_{Bob} \oplus \delta_{Alice})). \qquad (9)$$

If the mismatching rate $\epsilon$ is lower than the error-correcting ability of $C$, an appropriate ECC $C$ can be employed to ensure that $K'_{Alice} = K_{Alice}$. Therefore, both Alice and Bob agree on the same key $K'_{Alice} = K_{Alice}$, and they use the key to encrypt/decrypt the communication between them.

# 密钥生成

**3.防篡改——MAC（message authentication code）**



—To ensure the message $\delta_{Alice}$ is indeed sent from Alice, Alice sends a MAC message with $\delta_{Alice}$; the overall message sent by Alice is $L_{Alice} = \{\delta_{Alice}, MAC(K_{Alice}, \delta_{Alice})\}$. After receiving $L_{Alice}$, Bob computes $K'_{Alice}$ by Equation (9) and uses it for MAC verification. If Bob obtains $MAC(K_{Alice}, \delta_{Alice}) \neq MAC(K'_{Alice}, \delta_{Alice})$, he can conclude that the message was not sent by Alice, indicating the presence of an adversary.

—If Bob does not detect the presence of an adversary, he computes $\delta_{Bob}$ and transmits the following message to Alice: $L_{Bob} = \{\delta_{Bob}, MAC(K_{Bob}, \delta_{Bob})\}$.

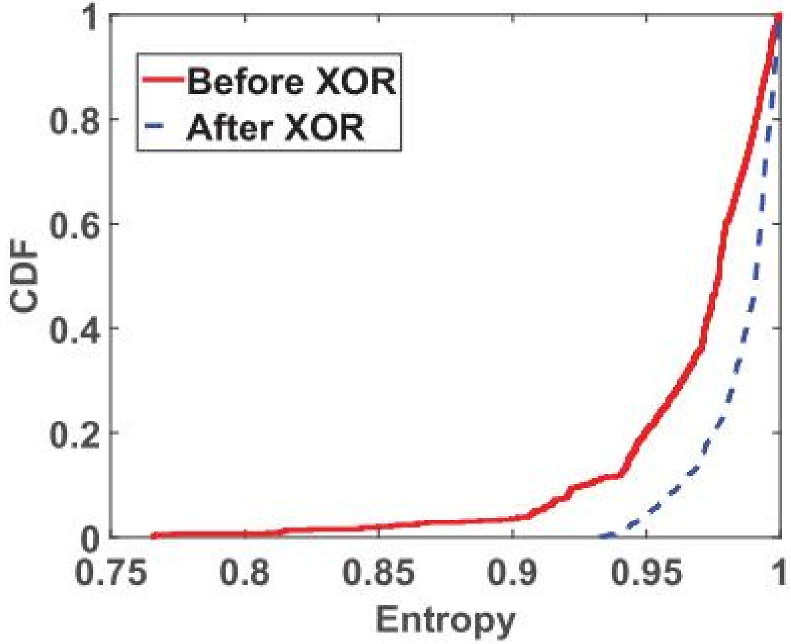
—Upon receiving $L_{Bob}$, Alice computes $K'_{Bob}$ and uses it for MAC verification. If Alice obtains $MAC(K'_{Bob}, \delta_{Bob}) = MAC(K_{Bob}, \delta_{Bob})$, she can confirm that the message was indeed sent by Bob. Since Eve does not know the bits in $K_{Bob}$ generated by Bob (he can just listen to the output of the $MAC(K_{Bob}, \delta_{Bob})$), modifying $\delta_{Bob}$ will fail the MAC verification at Alice.

# 密钥生成

## 4.隐私放大

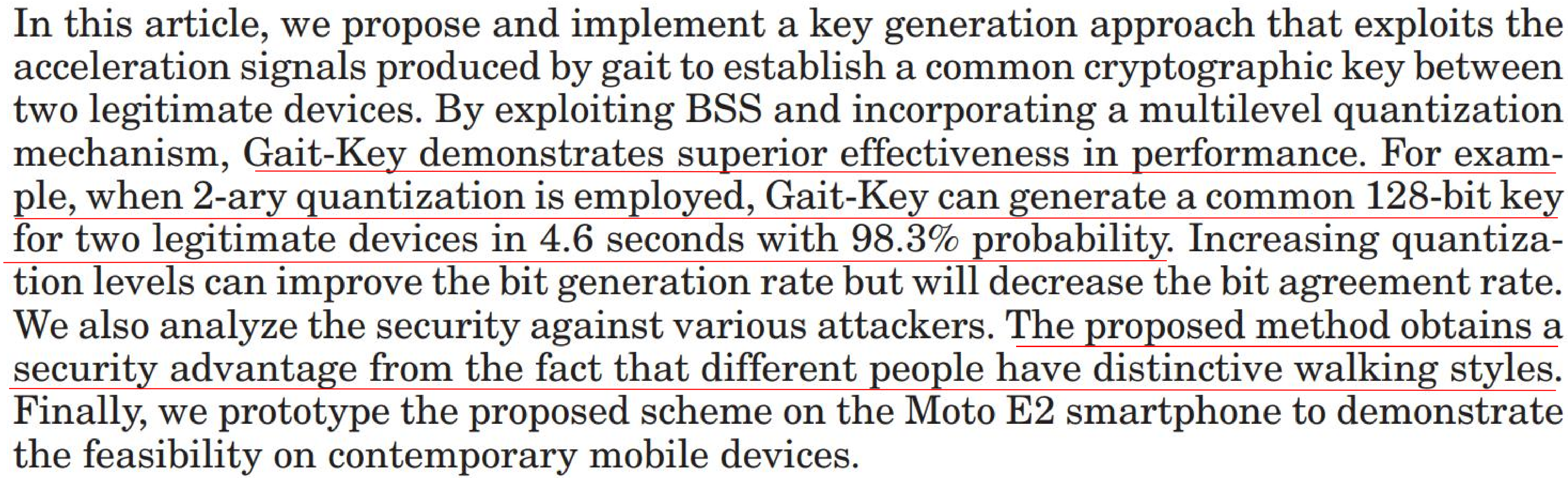
在系统中，我们使用**位异或函数**来组合各个方向生成的键，消除它们之间的相关性，减少了透露给敌手的相关信息。

经过隐私放大后，最终密钥可以被诸如AES之类的对称密钥算法使用，以确保Alice和Bob之间的安全通信。如果最终密钥的长度大于128位，则使用前128位。



(d) Impact of privacy amplification

# Conclusion



In this article, we propose and implement a key generation approach that exploits the acceleration signals produced by gait to establish a common cryptographic key between two legitimate devices. By exploiting BSS and incorporating a multilevel quantization mechanism, Gait-Key demonstrates superior effectiveness in performance. For example, when 2-ary quantization is employed, Gait-Key can generate a common 128-bit key for two legitimate devices in 4.6 seconds with 98.3% probability. Increasing quantization levels can improve the bit generation rate but will decrease the bit agreement rate. We also analyze the security against various attackers. The proposed method obtains a security advantage from the fact that different people have distinctive walking styles. Finally, we prototype the proposed scheme on the Moto E2 smartphone to demonstrate the feasibility on contemporary mobile devices.

感谢聆听 ☺