life.augmented

STM32 生态系统 第十二期

信息安全 . Information Security

03. 密码学基本原理（中）

2020.03

本期内容概览

1 哈希函数

2 完整性和安全性

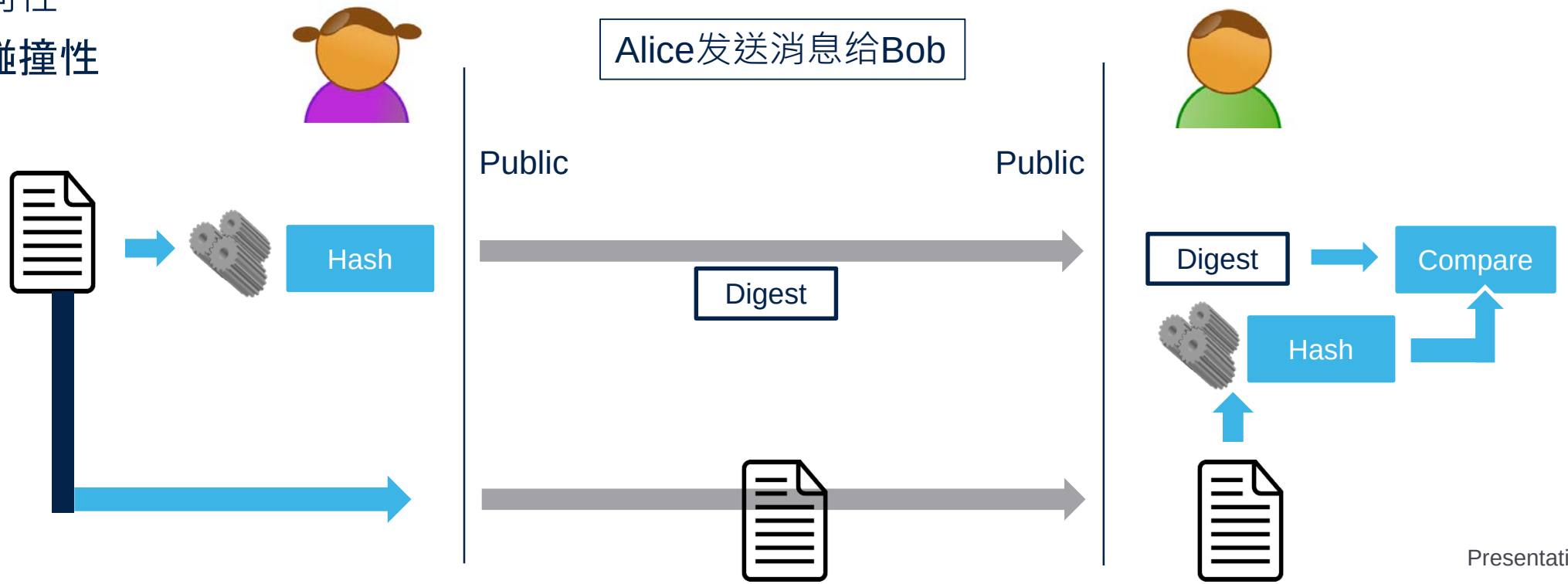
3 消息验证

4 常用算法

life.augmented

Hash/哈希/散列/摘要 函数

- **哈希函数的功能**：对任意输入可以产生固定长度的摘要值(Digest)
- **哈希函数的特点**
  - 输入的任何改变，都会导致摘要值变化
  - 单向性
  - **低碰撞性**

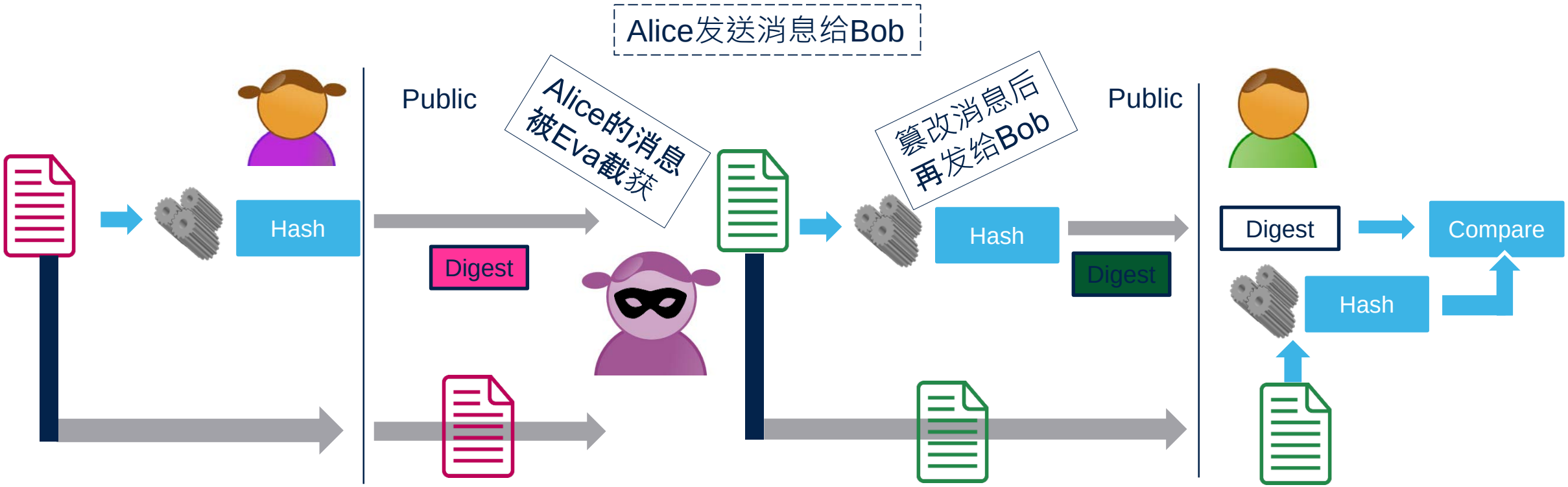


常用哈希算法

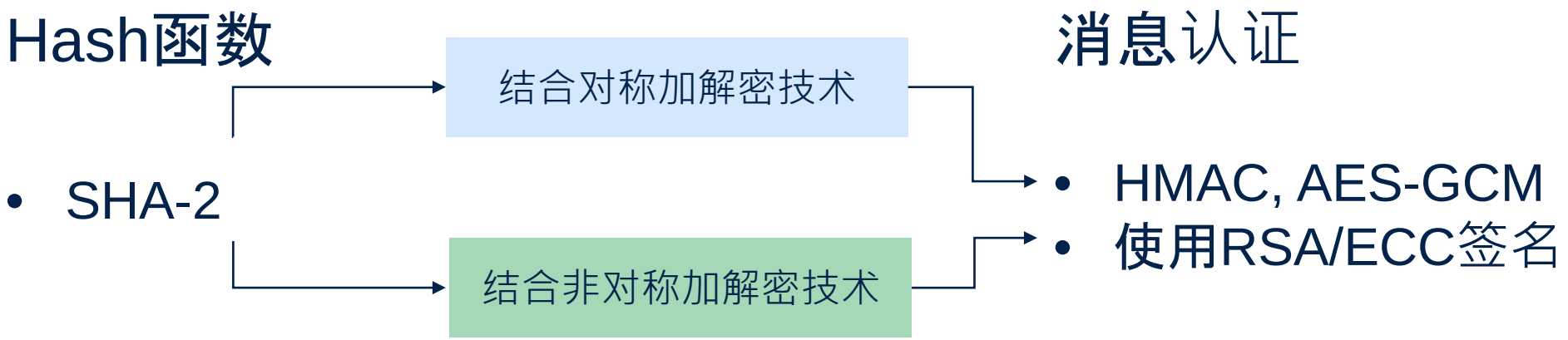
算法	模式	摘要值大小	说明
MD5 (Message Digest 5)		128 位	已被破解，不安全，不推荐使用
SHA-1 (Secure Hash Algorithm 1)		160 位	
SHA-2	SHA-224	224 位	
	SHA-256	256 位	
	SHA-384	384 位	
	SHA-512	512 位	
SHA-3		224 位	2015 US NIST标准
		256 位	
		384 位	
		512 位	

消息的“狭义完整性” 和“广义完整性”

- **哈希函数**，仅能保证消息的狭义完整性
- **要保**证数据确实是Alice发送的，需要消息认证机制/message authentication



消息认证/Message authentication



狭义
完整性

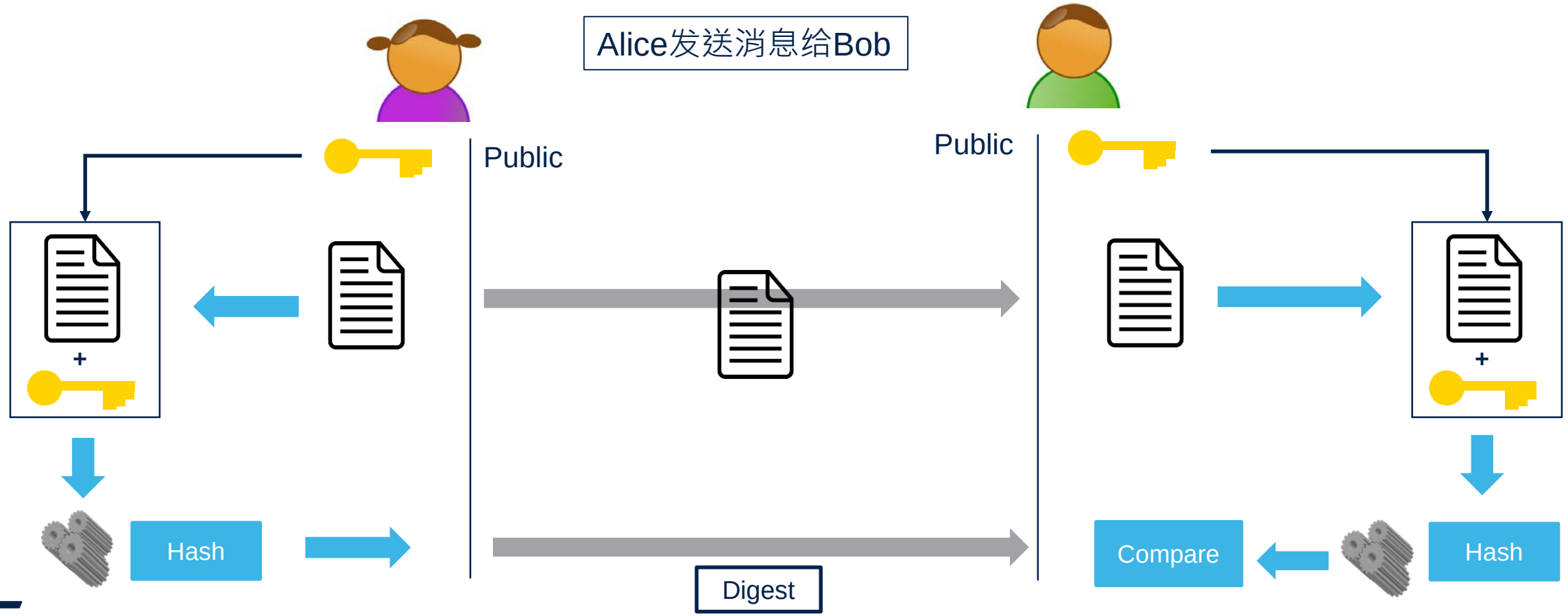
消息没有改变

消息确实是期望
的发送方发过来的

广义
完整性

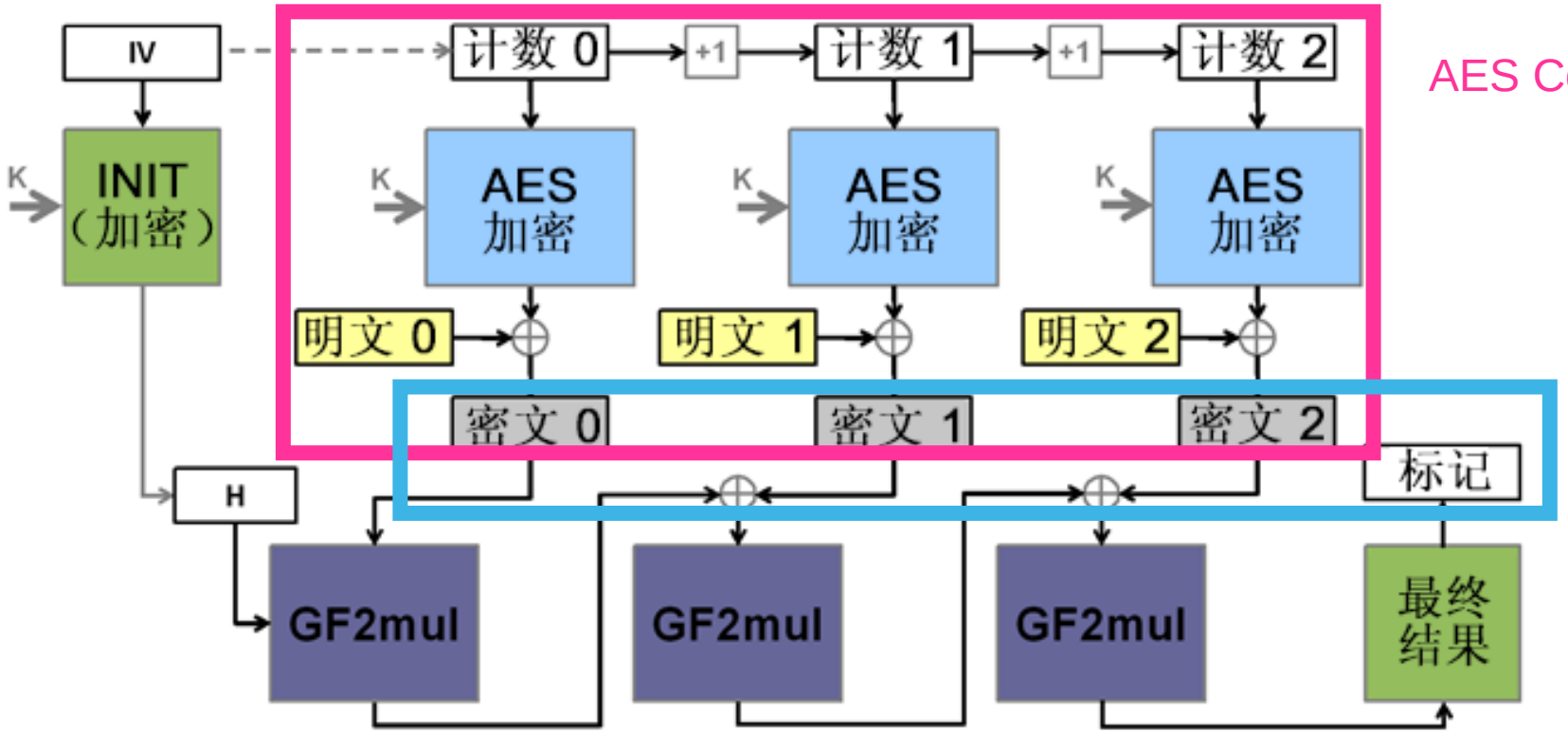
哈希和对称加解密技术的结合之一：HMAC

- **前提：双方事先**约定好一个共享密钥



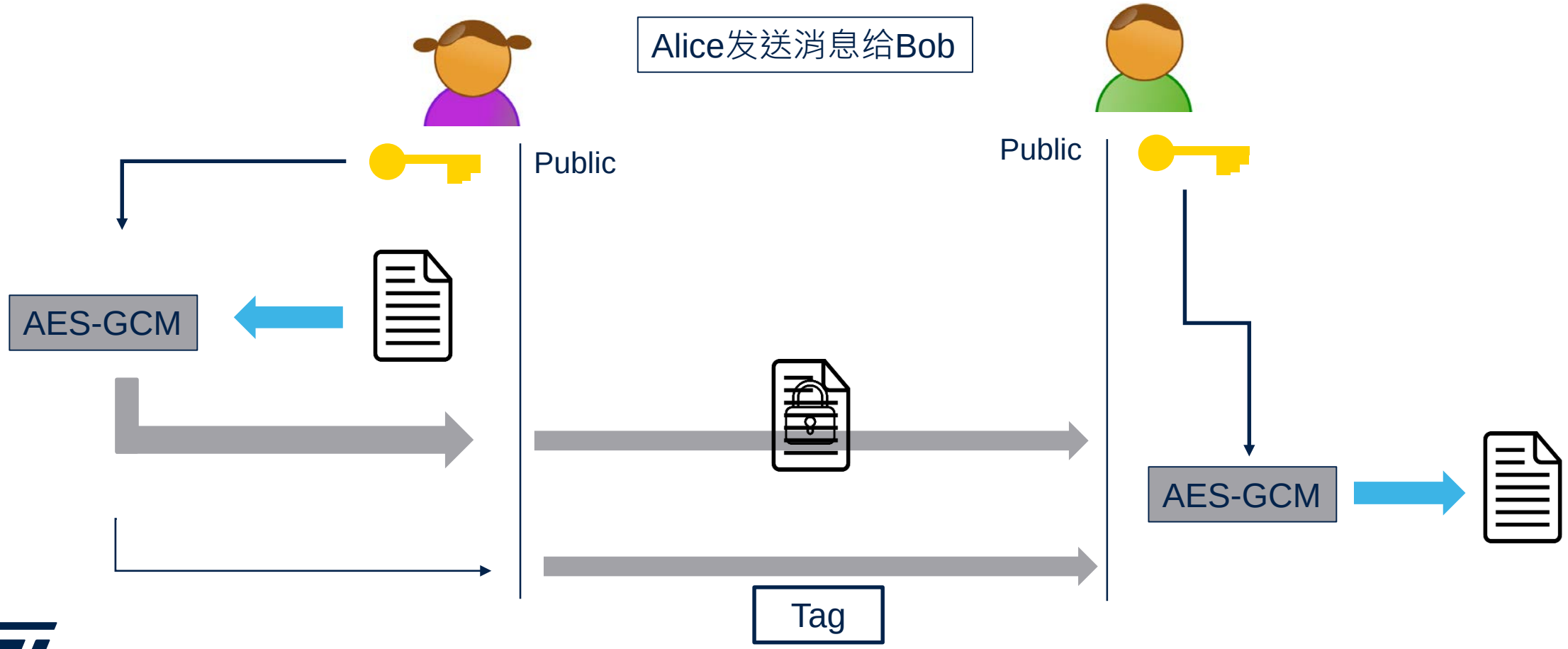
哈希和对称加解密技术的结合之二：AES - GCM

- AES counter模式 + 特殊的哈希
- 输出结果：加密后消息，该消息的认证码标签/tag



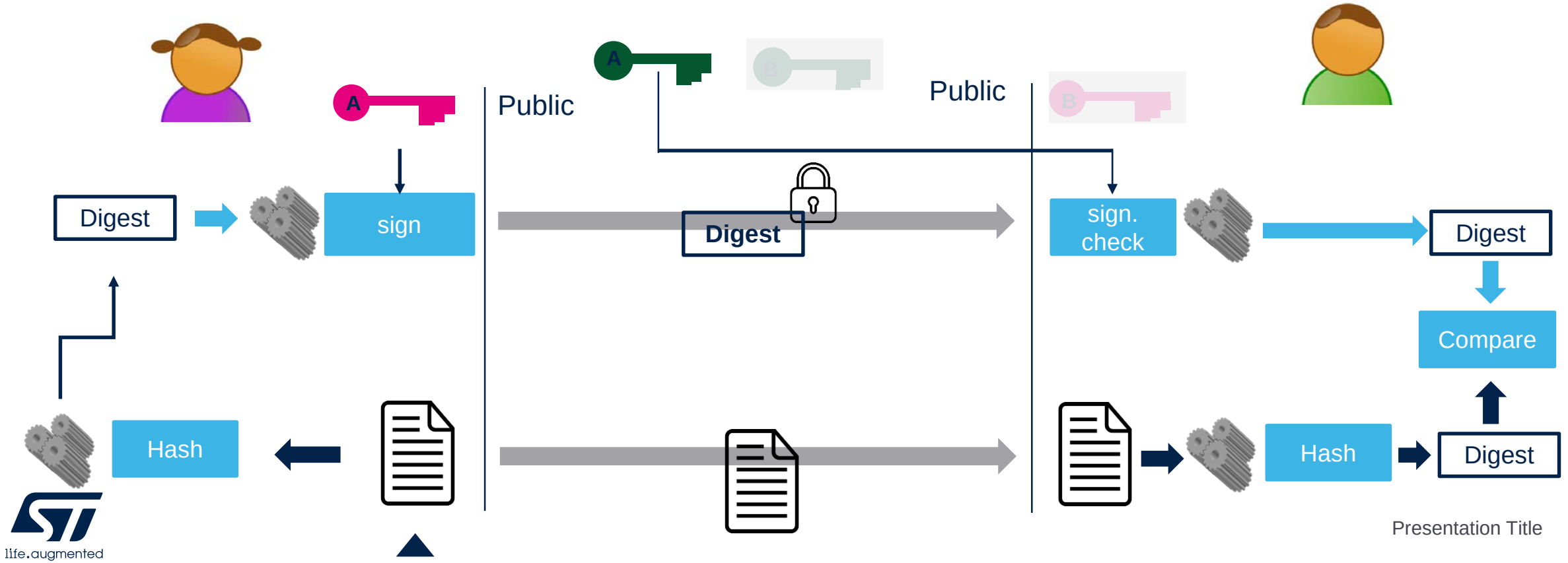
哈希和对称加解密技术的结合之二：AES - GCM

- **前提：双方事先**约定好一个共享密钥



哈希和非对称加解密技术的结合：签名

- Alice使用自己的私钥，把要发给Bob的消息的摘要进行加密（其实并没有保密）
- 以上操作定义为：Alice对消息签名



life.augmented

本期回顾

- **基本原理**

  哈希函数

  完整性和安全性

  消息认证

- **常用算法**

  对称加解密：**HMAC、AES-GCM**

  非对称加解密：**RSA/ECC签名**

谢　谢

life.augmented