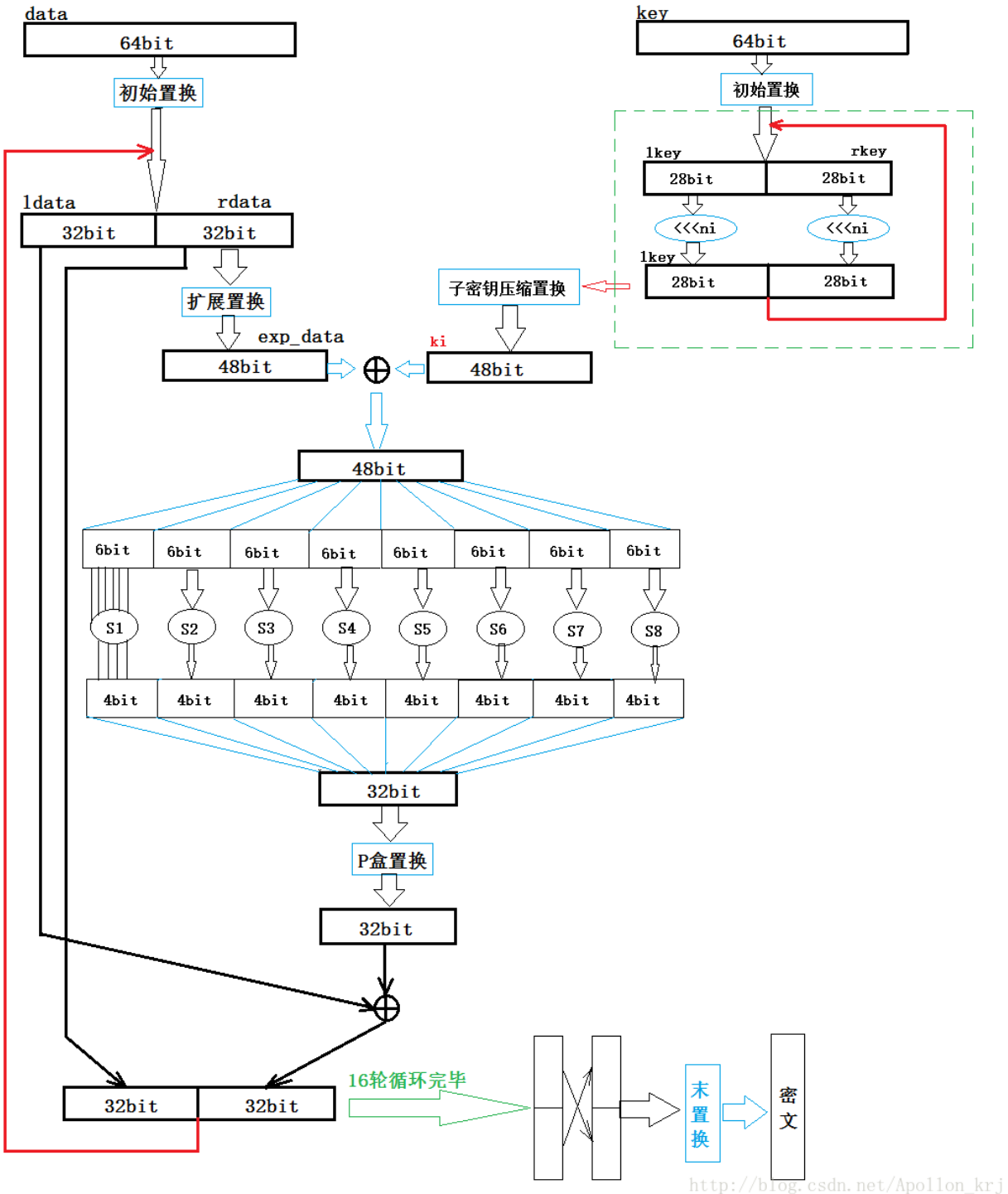
单向加密算法

- DES ，数据加密标准，速度较快，适用于大量数据
- 3DES，基于DES，用一块数据用三个不同的密钥进行加密
- AES 高级加密标准，支持128，192，256，512位的密钥加密

非对称加密：一个公钥一个私钥。没有对称加密的速度快

DES算法的工作流程：



首先由于DES是16轮循环，所以需要由64bit的随机密钥Key生成16个子密钥Ki（i从0~15），Key共64bit，但是其每个字节的最后一位都用不到（即第8、16、24、32、40、48、56、64位共8位），所以先通过初始置换将64bit的密钥转换为56bit。

RSA加解密原理

RSA公钥密码体制描述如下：（m为明文，c为密文）

1. 选取两个大素数p,q。p和q保密
2. 计算n=pq，r=(p-1)(q-1)。n公开，r保密
3. 随机选取正整数1<e<r，满足gcd(e,r)=1.e是公开的加密密钥
4. 计算d，满足de=1(mod r).d是保密的解密密钥
5. 加密变换:　　c=m^e mod n
6. 解密变换:　　m=c^d mod n

密码学应用安全技术体系的探讨

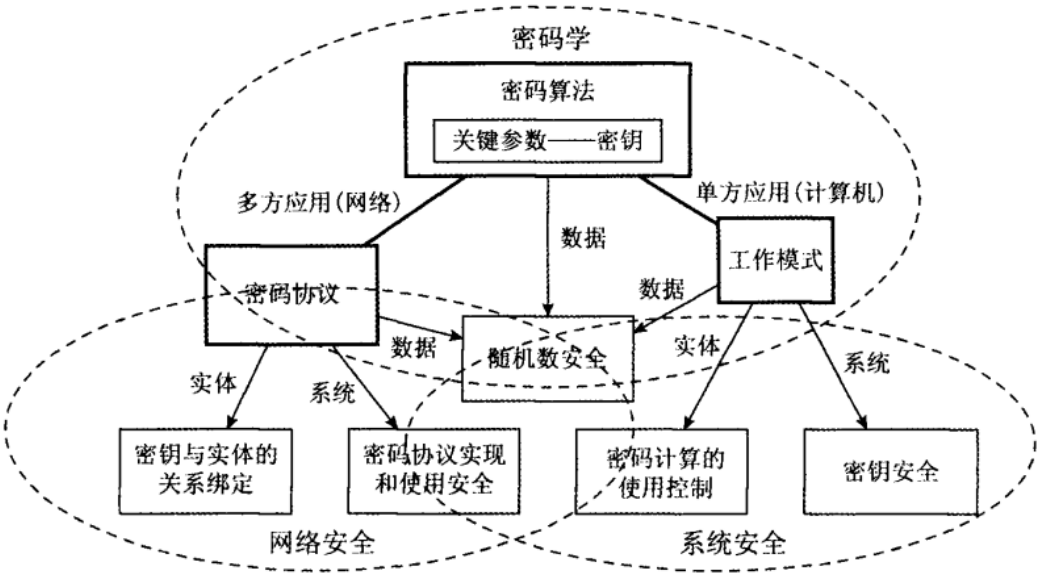


图 1　密码应用安全技术体系

对于密码算法，从数据安全角度而言，

- 最重要的是**密钥数据应源自随机数**，保证攻击者不可预测。
- 各种密码算法工作模式和密码协议通常也需要安全的**随机数**作为执行过程中的参数
- 在密码协议的设计和分析中，通常使用**不同的密钥来区分不同的实体**，密钥和实体之间的关系绑定直作为基本假设。
- 保证攻击者不能读取访问密钥，以满足密码算法最基本的要求

因此可以得出以下结论

1. 我们需要选择正确合适的密码算法，工作模式和密码协议
2. 维护合理的密钥参数
3. 产生安全的随机数
4. 用正确的方式实现和使用密码协议
5. 将密钥跟实体进行绑定
6. 确保密钥安全

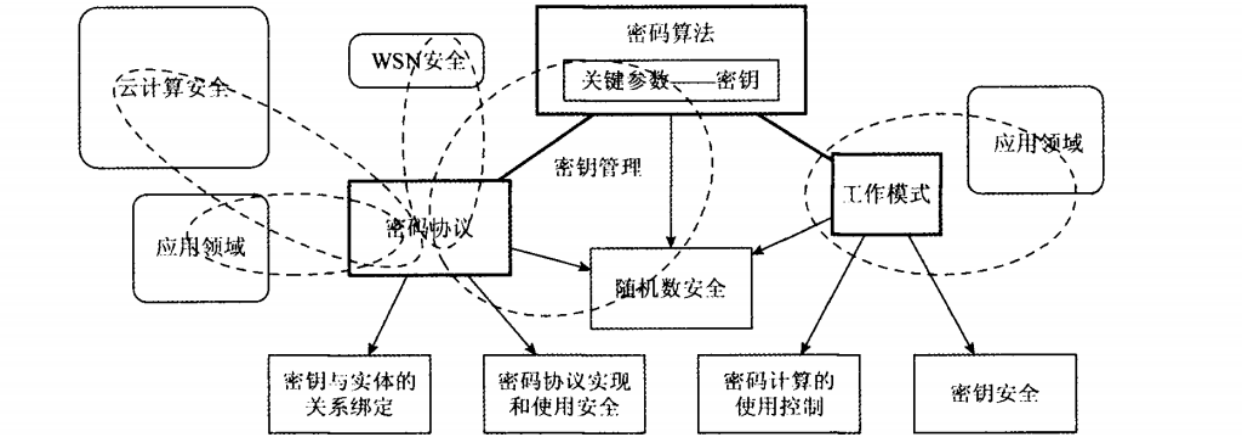


图 2　密码应用安全技术体系与现有研究方向