

USB Key 在 CPK 中的应用



1 CPK 简介

CPK (combined public key 组合公钥), 是一种利用椭圆曲线 (ECC) 算法 (但不限于该算法), 采用传统对称密码体制中的密钥管理中心 (KMC) 思路, 定义的一种公钥体制。它的最大特点就是可以通过有限的种子变量, 产生几乎无限的密钥对^①。用户使用该体制, 将不再需要 CA, 也不需要证书, 更不需要维护密钥库和证书吊销列表, 用户间的信任关系变得极其简单, 从而弥补了 PKI 在信任管理和密钥管理方面的不足。

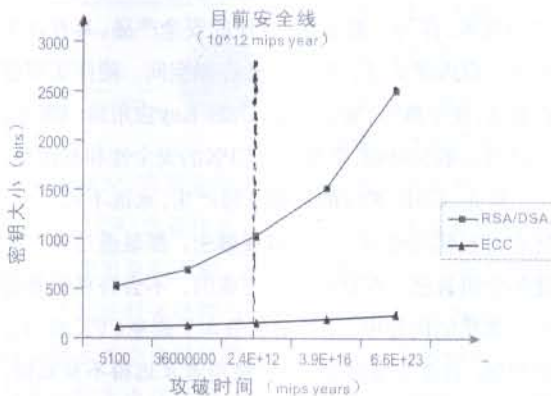
PKI 体系中, 用户使用两种不同的密钥: 公钥, 概念上存储在电子库中; 私钥, 通常存储在端用户的 pc 或是单独的智能卡等载体上。用公钥加密的数据只能采用相应的私钥解密。PKI 的密钥管理机构是可选的, 包括认证中心 CA (必须的) 和注册中心 RA (可选的)。认证中心 (CA) 通过将用户或系统身份绑定到公钥上的数字签名算法生成数字证书。CA 还有以下责任: 分发数字证书; 确定过期时间; 在必要时撤回证书。当密钥量较大时, 密钥的管理变得非常困难。另外 RA+CA 模式允许在内容上非权威的某种实体 (CA) 伪造证书, 可以认为 RA+CA 模式绝对不如密钥管理中心 (KMC) 方式安全。

CPK 体制中, 用户拥有私钥和公钥种子矩阵。CPK 的密钥管理机构只有 KMC, 所有的密钥由 KMC 来管理 (产生、分发、更换), 所有用户只需要信任 KMC 即可, 关系变得很简单。当用户需要使用公钥时, 通过系统预先定义好的计算方法, 可以由公钥种子矩阵计算出所需要的公钥。当然, 这种计算是基于种子组合的, 由于组合爆炸效应的存在, 就实现了前面提到的“通过有限的种子变量, 产生几乎无限的密钥对”。

举例来讲, 假设公钥种子矩阵是一个 256 行, 每行 32 个种子的矩阵, 则可组合的密钥量为 $256^{32} = 2^{256} \approx 10^{77}$, 这几乎是一个天文数字。

2 CPK 的安全性

CPK 的安全性, 依赖于它使用的 ECC 算法, 我们知道, ECC 安全强度不但依赖于在椭圆曲线上离散对数的分解难度, 也依赖于曲线的选择和体制, 目前 200 比特的椭圆曲线密码体制已经有了相当高的安全强度^②。



ECC与RSA的安全强度比较

从上图可看出, ECC 仅用短的密钥就可以达到 RSA 很长密钥的安全强度。目前, 大约 210 位的 ECC 就可以达到 2048 位的 RSA 的强度。

3 USB Key 在 CPK 中的应用思考

3.1 CPK 的问题

CPK 体制以简捷、高效、经济、可靠的方式实现了密钥生成、密钥分发、密钥存储等关键技术, 特别适用于各种大型可信系统和实名系统。但是, CPK 体制也存在它自身的问题。

CPK 最大的问题是存在被有限个用户合谋作案, 攻破整个系统的可能。还举前面的例子, 一个 256×32 的私钥种子矩阵, 尽管可以产生几乎无限个私钥, 但通过多个私钥列出的方程组, 只要知道一定数量的私钥, 构成了 256×32 的线性无关组, 则方程就有解了。最极端的情况下, 只需要 $256 \times 32 = 8192$ 个私钥, 这些私钥列出的方程组恰好是线性无

关组,那么就可以求出整个私钥种子矩阵,从而攻破整个系统。

CPK还有一个问题是KMC方式的普遍存在的,就是密钥的更换很困难。同一系统内的密钥,都是由种子矩阵计算出来的,如果需要更换种子矩阵,那么工程量和复杂度将随着系统用户规模的增大而巨增。有没有切实可行的密钥更换方案,是CPK能否顺利实施的一个重要问题。

3.2 USB Key 在 CPK 中可能的应用

USB Key结合了现代密码学技术、智能卡技术和USB技术,作为一款成熟、方便的安全产品,具有以下优点:双因素认证、带有安全存储空间、硬件实现密码算法、便于携带,安全可靠。USB Key应用到CPK中,正好可以取长补短,全面提升CPK的安全性和易用性。

首先,USB Key的私钥一经产生,永远不可导出,所有对私钥的使用,如签名或解密,都是通过硬件内置的密码算法,在硬件内部完成的,不会将私钥暴露到计算机的内存中。这样就从根本上避免CPK最担心的问题:合谋作案问题。因为使用者永远得不到私钥,更不可能利用私钥来列方程组,求解私钥种子矩阵了。分发密钥时,由KMC直接将产生的用户私钥和公钥种子矩阵,一起存放到USB Key中,将USB Key发给最终用户。当用户的USB Key损坏或者丢失以后,KMC可以很方便地给用户重新发放一个USB Key。整个过程非常简单、可靠。

其次,利用USB Key的安全存储空间,可以将公钥种子矩阵存储在USB Key中,这样方便用户随身携带,随时使用。同时,USB Key具有双因素认证的优点,可以给用户带来更好的安全体验。目前,主流的USB Key已经具备64K的安全存储空间,可以存储很大的公钥种子矩阵,也就是说,USB Key已经有能力应用到非常大型的系统中。

最后,使用USB Key可以简化密钥的更换工作。由于USB Key内置密码算法,需要更换系统密钥时,只需要将新的用户私钥和新的公钥种子矩阵,用指定用户的旧公钥加密后,发给用户(传送数据的通道,不要求是安全通道,因为数据是经用户公钥加密过的,即使被截获,也不可能存在安全威胁)。用户通过USB Key预先定义的更新接口,利用硬件内置的密码算法,就可以方便地更换密钥了。

4 结论

任何一种体制、一种方案,都有其特定的应用领域,只用一种方案解决所有的问题是不切实际的。正如本文所述,在某些应用领域,CPK有着自身特有的优势,即简单、易行、经济、高效。特别是USB Key在CPK中很好地应用之后,更进一步提升CPK的安全性和易用性。我们有理由相信,USB Key将伴随着CPK,在各种可信系统,如国防网、政府网、公安网、票据网、金融交易网、电子商务网等得到越来越广泛的应用。

参考文献

- ① 南湘浩,陈钟《网络安全技术概论》
- ② IEEE P1363 / D13 (Draft Version 13), 1999

