**CPK标识密钥**

**一、CPK编制特点**

**二、CPK密钥保护**

物联网的发展，给公钥体制提出了新的要求和新的挑战。物联网将过去user to user 的用户鉴别技术提高到identity to identity 的实体鉴别技术，过去以专网保密为主的安全技术改变为以公网真假判别为主的安全技术。

量子计算机的出世，也给传统的公钥体制提出了新的挑战，迫使人们采用使穷举运算失效的新技术。对数学来说，解决这样的问题并不是很困难的，因为穷举只有存在判别条件时才有意义。

CPK是基于标识的公钥体制。公钥体制提供数字签名和密钥加密两个功能。我们依靠CPK数字签名技术解决了标识鉴别的难题，在万物对万物的庞大而复杂的网络环境中，搭建了I to I的虚拟网络，提供可证连接。给物联网技术的可持续发展打下了良好的技术基础。

物联网上各种业务的需求各部相同，如办公需求、支付需求、防伪需求等。如果办公需求、支付需求、通信需求是一种要求，那么防伪需求、软件识别需求则是另一种要求。后一种，对大部分用户来说不需要使用私钥。

为了满足各种不同需求，CPK 组合公钥可以用芯片实现也可以软件实现。密钥长度可从112-256任选。签名长度是密钥长度加或5字节校验码构成。如密钥长度为192时，签名长度24加5等于29字节。

无论是CPK-chip或CPK-soft，其关键问题在于系统保护。从系统安全性角度开看，chip具有soft不可比拟的优势，一是使动态跟踪不可能，二是有些变量外部读不出，三是以并行计算可减少系统开销。如果软件能做到使动态跟踪无意义，使读出来的变量无意义，即不怕被窃、不怕被复制，那么软件也是安全的。由于全部用软件实现，其密钥管理可以在网上进行，不仅为大规模的使用提供了方便，而且结合网络的自动化动态管理的特点，可以提高系统运行安全的可能性。无论是硬件或软件，绝对防止静态分析是不可能的，因此，如何把握这个“度”是需要深入讨论的问题。有人说过：“理想的密码不好用，在用密码都有缺陷”。体制不是越安全越好，而是满足需求的是最好的。

CPK可做成芯片产品、也可做成软件产品，可以构成公众网，也可以构成专用网，密钥长度可选，可根据需要选型。

**2.1 系统保护**

CPK系统密钥由系统外部由用户定义的主密钥(口令pwd)和系统内部由随机数定义的随机主密钥(R1)以及由中心定义的年度密钥对，年度公钥(*YEAR*)和年度私钥(*year*)构成，共同保护系统安全。

**2.1.1 随机主密钥**

随机主密钥R1和保护主密钥的参数，由中心定义。随机参数个系统互不相同。保护随机主密钥R1的参数表（举例）如下：

参数表1：

AA=*ad*-1\**ac*-1

AB=*ae*\**ab*

AC=a*c*\**ae*-1

AD=*aa*-1\**ab*-1

AE=*ad*\**ae*\*R1

参数表是在口令加密下发放的，如：

Epwd(AA)=v1; Epwd(AB)=v2; Epwd(AC)=v3; Epwd(AD)=v4; Epwd(AE)=v5;

出厂时的口令是由厂家定义的，因此在系统正式启用时首先要换口令。口令的更换，系统提供更换协议。

CPK开机口令是口令句(pass phrase)，长度不限。口令句经Hash变换，变成机器口令pwd。

HashHkey(pass phrase)=pwd

当口令输入后，先对参数vi脱密：

Dpwd(vi)=AA..AE

计算R1：

AE\*AC\*AA=R1

检查口令的合法性：

**E**R1(R1)⊕R1 = *Z’*;

将*Z’*和系统中保有的*Z*相比较，如果正确，则进入下一步。口令连续5次不符，算一次安全事故，并将参数*Z*置“0”。

**2.1.2 年度密钥**

一年一度，由中心定义年度公钥*YEAR*和年度私钥*year*，年底网上发送，自动安装。年度密钥全网统一, 参数变量可随机定义。保护年度公钥*YEAR*的参数表（举例）如下：

参数表2：

BA=*bd*-1\**bc*-1

BB=*be*\**bb*

BC=*bc*\**be*-1

BD=*ba*-1\**bb*-1

BE=*bd*\**be*\**YEAR*

年度公钥在随机主密钥(R1)的保护下存放，如：

ER1(BA)=w1; ER1(BB)=w2; ER1(BC)=w3; ER1(BD)=w4; ER1(BE)=w5;

年度私钥*year*的发送和保护同上年度公钥。

参数表3：

CA=*cd*-1\**cc*-1

CB=*ce*\**cb*

CC=c*c*\**ce*-1

CD=*ca*-1\**cb*-1

CE=*cd*\**ce*\**year*

年度私钥在随机主密钥(R1)的保护下存放，如：

ER1(CA)=x1; ER1(CB)=x2; ER1(CC)=x3; ER1(CD)=x4; ER1(CE)=x5;

**2.1.3 通道密钥**

在系统发放时，每一系统随机法分配一个通道号Channel-no, 并配发公私钥对*CHANNEL-NO*和*channel-no*，专用于密钥的传递。*CHANNEL-NO*的参数表（举例）如下：

参数表4：

DA=*dd*-1\**dc*-1

DB=*de*\**db*

DC=*dc*\**de*-1

DD=*da*-1\**db*-1

DE=*dd*\**de*\**CHANNEL-NO*

通道公钥在随机主密钥(R1)的保护下存放，如：

ER1(BA)=y1; ER1(BB)=y2; ER1(BC)=y3; ER1(BD)=y4; ER1(BE)=y5;

通道私钥的存放形式同上通道公钥。

参数表5：

EA=*ed*-1\**ec*-1

EB=*ee*\**eb*

EC=e*c*\**ee*-1

ED=*ea*-1\**eb*-1

EE=*ed*\**ee*\**channel-no*

通道私钥在随机主密钥(R1)的保护下存放，如：

ER1(EA)=z1; ER1(EB)=z2; ER1(EC)=z3; ER1(ED)=z4; ER1(EE)=z5;

**2.2 标识私钥**

**2.2.1 签名私钥**

Alice的签名函数：

SIG*alice* (h) =(*s*, *c*)

其中，SIG是签名函数，*alice*是组合私钥，h是签名对象，如实体标识、日时组或数据的Hash码等，*s*是签名码，*c*是核对码。

在数字签名协议中私钥(*alice)*保护参数组，参数组的参数值随机定义，各系统间不互不相同。如：

参数表6：

FA=*fd*-1\**fc*-1

FB=*fe*\**fb*

FC=*fc*\**fe*-1

FD=*fa*-1\**fb*-1

FE=*fd*\**fe*\**alice*

年度签名私钥在随机主密钥(R1)的保护下存放，如：

ER1(FA)=q1; ER1(FB)=q2; ER1(FC)=q3; ER1(FD)=q4; ER1(FE)=q5;

Alice的签名过程如下：

首先将参数FE改为年度私钥参数FE’：

CE\*CA\*CC=ɑ

(FA\*FC\*ɑ)+FE=FE’

(由于FE’=fd\*fe\*(alice+year)=fd\*fe\*alice+fd\*fe\*year

其中FA-1\*FC-1=fd\*fc\*fc-1\*fe=fd\*fe)

Alice计算:

*c*=(*x*1+*y*1)2 mod 2*m*

*t*=*c*\*FA\*FC

*s* = *k*-1 (h + *t\**FE’) mod *n*

sign=(*s*,*c*)

Bob的验证不需要私钥，验证过程没有变化。

*s*-1hG+ *s-1* \**c \*ALICE*= (*x*1’, *y*1’)

= (*x*1’+*y*1’)2 mod 2*m*

**2.2.2 脱密私钥**

Bob的脱密函数：

DEC*bob*(β) =key

Dkey(code) = data

其中，DEC是非对称脱密函数，*bob*是私钥。

## 在脱中私钥保护参数形如：

参数表7：

GA=*gd*-1\**gc*-1

GB=*ge*\**gb*

GC=*gc*\**ge*-1

GD=*ga*-1\**gb*-1

GE=*gd*\**ge*\**bob*

年度脱密私钥在随机主密钥(R1)的保护下存放，如：

ER1(GA)=r1; ER1(GB)=r2; ER1(GC)=r3; ER1(GD)=r4; ER1(GE)=r5;

(注：在密钥加密参数表中，参数GA=*gd*-1\**gc*-1是全网公用的参数。

Alice 给Bob加密：

首先将参数GE改为年度脱密私钥参数GE’：

CE\*CA\*CC=ɑ

(GA\*GC\*ɑ)+GE=GE’

Alice加密：

ENC*BOB*(key)=β

η*=*β\*GA-1

msg={code, η}

Bob 脱密：

η \*GC-1\*GE-1=key

**2.3 私钥生成**

**2.3.1 标识私钥申请**

密钥的申请，通过通道密钥进行，而通道私钥在参数表5的保护之下，参数表5又在随机主密钥R1的加密下，因此先行脱密：

DR1(密参数表5)=名明参数表5

为了说明方便，签名协议和密钥加密均按通用表达式描述。首先要验明系统通道号的真实性。通道号真实性证明是通道号对申请时间的签名：

SIG*channel-no*(time)=(*s*1,*c*1)=sign1

任何标识都可以申请私钥，如电话号码、邮件地址等标识，网上可以直接证明其真实性，但实名、账号等，网上不能直接证明其真实性。比如Bob申请实名的私钥，则需要提出电话号码(phone-no)、身份证号码(ID-no)等证明实名(Bob)的证明。

SIG*channel-no*(phone-no)=(*s*2,*c*2)=sign2

SIG*channel-no*(ID-no)=(*s*3,*c*3)=sign3

SIG*channel-no*(Bob)=(*s*4,*c*4)=sign4

申请人按申请格式的要求，做成data1:

Data1={sign1,sign2,sign3,sign4}

申请人将data1用中心的公钥加密：。

*r*G=key1

Ekey1(data1)=code1

HASH (Center)→*i,j*; ∑(*Ri,j*)→ *CENTER*

ENC*CENTER*(key1)=β

申请人将加密后的数据发送给中心*CENTER*

msg1={code1,β}

其中，E是对称加密，ENC是非对称加密，*channel-no*是通道号私钥, *center*是中心的私钥，*CENTER*是中心的公钥。

密钥分发中心Center先行脱密：

DEC*center*(β)=key1

Dkey1(code1)=data1

中心检查申请的真实性：

VER*CHANNEL-NO*(time,*s*1)=*c*1’

VER*CHANNEL-NO*(phone-no,*s*2)=*c*2’

VER*CHANNEL-NO*(ID-no,*s*3)=*c*3’

VER*CHANNEL-NO*(Bob,*s*4)=*c*4’

密钥分发中心确认申请私钥的实名标识是Bob：

密钥管理中心生成Bob的私钥*bob’*:

HASHHkey1(Bob)→*i,j*; ∑(*ri,j*)→*bob’*

其中，DEC是非对称脱密函数，D是对称脱密函数，VER设验证函数，*CHANNEL-NO*是通道号的公钥。

中心生成Bob的私钥*bob’*以后，以用户通道公钥加密发送：

*r*G=key2

Ekey2(*bob’*)=code2

ENC*CHANNEL-NO*(key2)=beta

中心发送msg:

Msg={code2,beta}

**2.3.2其他参数保护**

Bob一旦有了自己的私钥*bob*，重新定义一个随机密钥，将重要参数重新加密。具体做法是：

随机定义一个随机数*r* ,计算*r*G=key，key则用于数据的加密，并用自己公钥*BOB*下加密存放。

Ekey(公钥矩阵)

Ekey置换表)

Ekey(Hkeyi)

ENC*BOB*(key)

**小结**

在开放环境下私钥的保护技术，不仅在CPK体制下有意义，对其他体制也有意义，它将大大降低私钥存储成本，并大大方便私钥的广泛使用。密钥的存储和调用方法，不仅适用于保密系统中