Open Access Library Journal
2021, Volume 8, e7440
ISSN Online: 2333-9721
ISSN Print: 2333-9705

New Progress in CPK Public Key

Xianghao Nan

CPK Lab, Beijing, China
Email: nanxianghao@bochtec.com

How to cite this paper: Nan, X.H. (2021) New Progress in CPK Public Key. *Open Access Library Journal*, **8**: e7440.
https://doi.org/10.4236/oalib.1107440

Received: April 22, 2021
Accepted: August 16, 2021
Published: August 19, 2021

Abstract

The private-key structure of CPK has developed from single-layer and multi-layer to multi-block and composite structure. The scheme structure of CPK has formed as fixed, flexible or disposable types. CPK digital signature forms an identity signature protocol not only for data signature, but also for identity signature. CPK is not only suitable for the authentication requirements of open global communication network and business network, but also suitable for the authentication requirements of closed local communication network and business network. The disposable private-key structure can resist quantum exhaustion.

Subject Areas

Computer and Network Security

Keywords

Public Key, Signature, Authentication, Encryption, Mapping

1. 引言

CPK 鉴别系统由 CPK 组合公钥[1]和 GAP 一步协议[2]构成，为物联网的每一实体，为事联网的每一事件提供真实性证明。CPK 组合公钥是 CPK 鉴别系统的核心技术，而 CPK 的核心技术是标识鉴别。标识鉴别具有“事前证明”的性质，用于通信网络与业务网络的接入控制，有效防止非法接入。因此，“标识鉴别”成为各国梦寐以求的“银弹”。

用 CPK 组合公钥实现的“GAP 一步协议”是通用协议，实现“一物一证，一事一证”的当场鉴别，以阻断信任的转移和由此产生的权利的被接管，是对抗网络攻击和阻止黑客作案的有力武器。

2. CPK工作原理

CPK 在 ECC [3] [4]上实现，由组合矩阵和映射函数构成，矩阵分为私钥

矩阵 a 和公钥矩阵 A，分别用分别用 $a=\left(r_{i,j}\right)$ 和 $A=\left(R_{i,j}\right)$ 表示，r 是小于 n 的随机整数，私钥矩阵 $\left(r_{i,j}\right)$ 由 KMC 保有，用于私钥的生成，公钥矩阵 $\left(R_{i,j}\right)$ 由各客体保有，用于公钥的生成。公钥矩阵是由私钥矩阵派生的：$r_{i,j}*G=R_{i,j}$。

矩阵的坐标是由 YS 序列指示的，YS 序列是实体标识(Alice)在映射密钥 Hkey 作用下 Hash 输出。

$$\mathrm{YS}=\mathrm{Hash}_{\mathrm{Hkey}}\left(\mathrm{Bob}\right)=v_0,v_1,\cdots,v_{31}$$

v_i 的字长为 5 bit，$v_0,v_1,\cdots,v_{31}$ 指示行坐标，列坐标采用自然序。

3. 私钥结构

CPK 私钥的结构是从单层结构发展为多块性和而成性的。其中多块性具有普遍意义，而合成性是满足防量子穷举的特殊需要的。

3.1. 私钥的单层结构

原始的 CPK 的私钥是单层结构的，称 CPK v0.0 版本。

矩阵的坐标是由 YS 序列指示的：

$$\mathrm{YS}=\mathrm{Hash}_{\mathrm{Hkey}}\left(\mathrm{Bob}\right)=v_0,v_1,\cdots,v_{31},\cdots$$

Bob 的私钥由中心计算：

$$\mathrm{bob}=\sum_{i=0}^{31}r_{[v_i,i]}\bmod n$$

公钥则由验证方计算：

$$\mathrm{BOB}=\sum_{i=0}^{31}R_{[v_i,i]}$$

公钥可以大斜 BOB 表示，私钥以小斜 bob 表示。

显然，私钥是一个方程，方程带来什么危害，作为公开问题提出来。一般的理解是按代数定理，线性无关方程当满秩时导致唯一解，而线性相关方程导致无穷解。CPK 由于取值特点，不构成构成满秩矩阵，最大秩为 993。

3.2. 私钥的多层结构

在防量子穷举的研究中，为了增加解方程的难度，在私钥构成等式中增设了分层参数 fcc 和年度密钥 year，形成了 CPK v0.9 版本。

$$\mathrm{YS}=\mathrm{Hash}_{\mathrm{Hkey}}\left(\mathrm{Bob}\right)=v_0,v_1,\cdots,v_{31},v_{32},v_{33}$$

$$\mathrm{Fcc}_{\mathrm{Bob}}=:\left(v_{32}\times v_{33}\right)$$

Bob 的私钥由中心计算：

$$\mathrm{bob}=\left(\sum_{i=0}^{31}r_{[v_i,i]}\times\mathrm{fcc}_{\mathrm{Bob}}+\mathrm{year}\right)\bmod n$$

Bob 的公钥则由验证方计算：

$$\mathrm{BOB}=\sum_{i=0}^{31}R_{[v_i,i]}\times\mathrm{fcc}+\mathrm{YEAR}$$

年度公钥 YEAR 是单独公布的，全网相同。在分层参数的作用下，矩阵变成多层次的矩阵，方程变为多系数方程。

3.3. 私钥的多块结构

2016 年，廖国鸿等人发表了“组合公钥体制的线性共谋攻击”[5]的论文，对 CPK v0.0 实施了攻击，而获得成功。他们建立了秩为 993 的最大线性无关的等效矩阵，等价求出了 CPK 私钥矩阵，所用私钥为 3000 个。那么等效矩阵的线性攻击法很可能对 CPK v0.9 也有效，因为年度密钥是固定因素，他没有破坏矩阵的平移等价性，分层参数在一个私钥的等式中式固定的，而且可以被消掉。由此产生了私钥的多块结构，不仅消不掉分层参数，更使私钥方程变为参数保护下的两层无穷解方程。

由此将分层参数 fcc 由一个增加到 4 个，形成了多块结构的私钥，解决等价矩阵的建立，称 CPK v1.0。

$$YS = Hash_{Hkey}\left(Bob\right) = v_0, v_1, \cdots, v_{31}, v_{32}, v_{35}$$

$$fcc_{Bob}\left[i\right] =: \left(v_{i+32}\right)\left(i = 0 \cdots 3\right)$$

Alice 的私钥由密钥管理中心计算：

For j:= 0 to 3 do

$$alice\left[j\right] = \sum_{i=0}^{7} r_{\left[v_{i+j\times 8}, i+j\times 8\right]} \times fcc\left[j\right] \bmod n$$

$$alice = \left(alice\left[j\right] + year\right) \bmod n$$

Alice 的公钥由验证方算：

For j:= 0 to 3 do

$$ALICE\left[j\right] = \sum_{i=0}^{7} R_{\left[v_{i+j\times 8}, i+j\times 8\right]} \times fcc\left[j\right]$$

$$ALICE = \left(ALICE\left[j\right] + YEAR\right) n$$

3.4. 私钥的合成结构

设置两个中心，一是密钥管理中心，负责注册和第一密钥的分发；二是密钥服务中心，负责第二密钥的分发。第一密钥的公钥矩阵和 Hkey 公布，以便让客户计算第一公钥。

第一私钥由管理中心(KMC)生成：

$$\mathrm{Hash}_{\mathrm{Hkey1}}\left(\mathrm{Bob}\right) = v_0, v_1, \cdots, v_{15}, v_{31}, v_{32}, v_{33}$$

$$\mathrm{bob} = \left(\sum_{i=0}^{31} r_{\left[v_i, i\right]} \times \mathrm{fcc1}_{\mathrm{Bob}} + \mathrm{year}\right) \bmod n$$

第一公钥由客户计算：

$$\mathrm{Hash}_{\mathrm{Hkey1}}\left(\mathrm{Bob}\right) = v_0, v_1, \cdots, v_{31}, v_{32}, v_{33}$$

$$\mathrm{BOB} = \sum_{i=0}^{31} R_{\left[v_i, i\right]} \times \mathrm{fcc1}_{\mathrm{Bob}} + \mathrm{YEAR}$$

第二私钥由服务中心(SVC)生成：

$$\mathrm{Hash}_{\mathrm{Hkey2}}\left(\text{timed-Bob}\right) = w_0, w_1, \cdots, w_{31}, w_{32}, w_{33}$$

$$\mathrm{bob}'' = \left(\sum_{i=0}^{31} s_{\left[w_i, i\right]} \times \mathrm{fcc2}_{\mathrm{Bob}}\right) \bmod n$$

第二公钥由服务中心生成：

$$\mathrm{Hash}_{\mathrm{Hkey2}}\left(\text{timed-Bob}\right)=w_0,w_1,\cdots,w_{31},w_{32},w_{33}$$

$$\mathrm{BOB}''=\sum_{i=0}^{15}s_{[w_i,i]}\times\mathrm{fcc2}_{\mathrm{Bob}}$$

时刻私钥由客户合成：

$$\mathrm{bob}^{\#}=\mathrm{bob}+\mathrm{bob}''$$

时刻公钥由客户合成：

$$\mathrm{BOB}^{\#}=\mathrm{BOB}+\mathrm{BOB}''$$

由于第二私钥时刻化标识的作用下，使私钥具有一次性。

4. 编制结构

为了适应全局性开放环境中鉴别的需求，适应局域性封闭环境中鉴别的需求，以及防止量子计算穷举的特殊需要，定义了三种不同版本，固定型、灵巧型、一次型。

4.1. 编制的固定型

固定型适应全局性开放的通信网络和业务网络的鉴别需求，同时为加密数据提供密钥加密功能(不包括数据加密)。

矩阵大小固定为 32 × 32;

密钥长度固定为 256 bit;

分层参数的数量 固定为 4 个；

验证码长度固定为 $2^m = 2^{32}$。

固定型称 CPK v1.0。

4.2. 编制的灵巧型

灵巧型适应局域性封闭的通信网络和业务网络的鉴别需求；同时为加密数据提供密钥加密功能(不包括数据加密)。

矩阵大小范围为 4 × 4 … 16 × 16；

密钥长度的范围为 64 … 128；

分层参数数量 2 个；

验证码长度为 $2^m = 2^{16}$。

灵巧型称 CPK v1.1。

4.3. 编制的合成型

密钥管理中心和密钥服务中心各自生成一半密钥，由用户合成为一个密钥。合成型满足防量子计算攻击的特殊需求；同时为加密数据提供密钥加密功能(不包括数据加密)。

设置密钥管理中心，配置矩阵 1，大小为 32 × 32，设置和密钥服务中心，配置矩阵 2，大小为 32 × 32；两个中心配置不同的 Hkey1 和 Hkey2，密钥长度均为 256 比特；分层参数各一个，验证码长度为 $2^m = 2^{32}$。

一次型称 CPK v1.2。

5. 数字签名

CPK 的签名用修改的 DSA [6]实现。一般的数字签名只证明客体的真实性，如：

$$\mathrm{SIG}_{sk}(\mathrm{h})=(s,c);\ \ s=k^{-1}(\mathrm{h}+c*sk);$$

$$\mathrm{VER}_{PK}(\mathrm{h},s)=c';\ \ c'=s^{-1}(\mathrm{h}*\mathrm{G}+c*PK)$$

如果 $c=c'$，则证明 sk 和 PK 是一对密钥，因此客体 h 是真实的。至于谁签的名，则另行给出证明。但是用基于标识的公钥签名时，含义就发生变化。

5.1. 对客体的签名

CPK 的签名是签名方用由标识派生的私钥进行，验证是依赖方由标识派生的公钥进行，因此，签名与验证构成特殊的证明关系。举一个 Alice 对客体 h 签名的例子：

$$\mathrm{SIG}_{alice}(\mathrm{h})=(s,c);\ \ s=k^{-1}(\mathrm{h}+c*alice);$$

$$\mathrm{VER}_{ALICE}(\mathrm{h},s)=c';\ \ c'=s^{-1}(\mathrm{h}*\mathrm{G}+c*ALICE)$$

当 $c=c'$ 时，验证方可直接认定：

1) 签名所用私钥和验证所用公钥是一对的；

2) 标识和密钥是一体的，因为密钥是从标识派生的；进而直接验证标识的真实性；

3) 真实的标识对客体 h 签了名，因此 h 是真实的。

基于标识的公钥对客体的签名，不仅用于真实性证明，还可以用于所属性证明。在物理世界中，所属性可用占有性实现，但在逻辑世界中，很难实现占有性，因此所属性证明一直是难点。比如像数字货币，所属性应由逻辑方法解决，而不能采用纸质货币的钱包形式体现所属性。

5.2. 对标识的签名

在主体对客体签名的实例中可看出，在一次证明中，同时证明了标识真实性和客体真实性，但证明是有顺序的。在对客体的真实性判别依赖标识的真实性证明，即在客体真实性证明之前先进行标识的真实性证明，发过来，标识真实性证明与客体真实性证明无关。因此可另行构造标识签名协议。

$$\mathrm{SIG}_{alice}(0)=(s,c);\ \ s=k^{-1}c*alice$$

$$\mathrm{VER}_{ALICE}(0,s)=c';\ \ c'=s^{-1}c*ALICE$$

标识签名用于标识鉴别，标识鉴别不仅证明标识的真实性，更证明其声称要求的真实性。比如一人声称他是张三，并提供标识签名的证据，那么，证明了他就是张三，也证明了他的声称权是真实性的。又比如，在数字货币中印有“中国人民银行”。这是一种声称，标识签名就可以解决。如果靠第三方证明，那么还要提供第三方真实性的证明。声称权的证明也可以用作溯

源性证明。

6. 结束语

从以上版本变化过程中可以看到，CPK 具有很好的结构特点很容易适应各种不同环境和要求。中国顶级密码和信息安全专家组成的评议会认为：“具有重大创新意义”[1]，国外专家认为“CPK 将公钥体制梦寐以求的所有好处集于一身”[2]。由于某些原因，CPK 在中国至今没被推广使用，不过到了物联网时代，会出现越来越多非使用 CPK 不可的情况，也会有越来越多的人认识到 CPK 的使用价值。

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] 南湘浩, 陈钟. 网络安全技术概论[M]. 北京: 国防工业出版社, 2003.

[2] 南湘浩. GAP 一步鉴别协议[J]. 通信技术, 2020, 53(12): 3030-3033.

[3] Standard for Efficient Cryptography (2000) SEC1: Elliptic Curve Cryptography. https://www.secg.org/SEC1-Ver-1.0.pdf

[4] Standard for Efficient Cryptography (2000) SEC2: Elliptic Curve Cryptography. https://www.secg.org/SEC2-Ver-1.0.pdf

[5] 廖国鸿, 等. 组合公钥体制的线性共谋攻击[J]. 计算机应用与软件, 2016, 33(12): 291-294.

[6] National Institute of Standards and Technology (1994) FIPS PUB 186, Digital Signature Standard (DSS), U.S. Department of Commerce. https://www.govinfo.gov/app/details/GOVPUB-C13-68d0348eda62ce4d62288b92c211bac9

Appendix (Abstract and Keywords in Chinese)

CPK 组合公钥的新进展

摘要：CPK 的私钥结构由单层、多层发展到多块和合成结构；CPK 的编制结构形成为固定型、灵活型、一次型；CPK 数字签名不仅对数据签名，也可对标识签名，形成了标识签名协议，不仅提供真实性证明和溯源性证明，还提供普通数字签名难于实现的声称权证明和所属性证明。CPK 不仅适用于开放的全局性通信网络和业务网络的鉴别需求，还能适应于封闭的局域性通信网络和业务网络的鉴别需求；其中合成性私钥结构能抵抗量子的穷举。

关键字：公钥，签名，鉴别，加密，映射

[1]2005 年 6 月 3 日北京市科技技术委员会专家评议意见。

[2]James P. Hughes (2013) Preface to “CPK Cryptosystem and Identity Authentication—Basic Technology of Active Management”.