一个基于双线性对的前向安全的代理签名方案

夏祥胜 洪 帆 耿永军 崔国华
(华中科技大学计算机科学与技术学院 武汉 430074)

摘 要 提出了一个基于双线性对的前向安全的代理签名方案,方案能实现即使代理签名人的密钥被泄露,之前所产生的代理签名依然有效。该方案是基于双线性签名体制构造的,具有签字短、安全、高效等优点,不仅能有效抵制任何第三方和原始签名人的伪造攻击和代理签名人的代理权滥用,而且能满足强代理的一切性质。最后,对所提出方案的安全性做了详细分析和讨论。

关键词 前向安全,强代理签名,双线性对,安全分析

Forward Secure Proxy Signature Scheme Based on Bilinear Pairings

XIA Xiang-sheng HONG Fan GENG Yong-jun CUI Guo-hua
(School of Computer Science, Huazhong University of Science & Technology, Wuhan 430074, China)

Abstract A forward secure proxy signature scheme based on bilinear pairings was proposed. In the scheme, the former proxy signature is still valid even if the secret keys of proxy signers are lost. The scheme is based on bilinear pairings, which can make signature short, secure and efficient. The scheme can not only effectively resist the forgery attacks from any third party and original signer's and misusing of the proxy signature right from proxy signers, but also satisfies all security properties of strong proxy signature. Finally, the security of the proposed scheme was analyzed and discussed in details.

Keywords Forward security, Stong proxy signature, Bilinear pairings, Security analysis

1996年,Mambo等人首次提出了代理签名方案[1,2]。在一个代理签名方案中,一个被指定的代理签名人可以代表原始签名人生成有效的代理签名,一个验证人能够通过给定的步骤验证签名的有效性,从而可以相信签名是原始签名人同意并授权的。一个代理签名至少应满足可验证性、不可伪造性、可区分性、不可否认性等安全性质。

代理签名由于在电子现金、电子投票、移动代理及电子商务等方面有广泛的应用前景,一经提出便引起了人们的广泛关注。目前,已经有很多中外学者对代理签名进行了深入研究,已提出了很多种代理签名方案,如代理盲签名[3]、代理多重签名[4]、门限代理签名[5]等等。然而,当签名人的代理密钥泄露后,以前的代理签名就变得不可信赖。1997年,R. Anderson首次提出了前向安全的概念[6]。前向安全就是把整个有效时间分成若干个周期,在每个周期内使用不同的签名密钥产生签名,而验证签名的公钥在整个有效时间内保持不变。即使当前周期的签名密钥被泄露,此周期之前所产生的签名依然有效,从而大大减轻了由于签名密钥泄露而对系统带来的不利影响。2005年,王晓明等首次将前向安全的概念引入代理签名体制[7]和代理多重签名[8],但王晓明的代理签名方案[7]是基于一般群上的离散对数体制构造的,而且后来被证明不具有前向安全性[9]。目前已提出许多前向安全的签名方案[10-12]。

双线性对作为一种构造密码学体制的工具,由于其签名短、安全、高效等优点,在密码学领域中引起了普遍的关注,并在数字签名中得到了广泛的应用[13-15]。本文基于双线性对构造了一个前向安全的代理签名方案,并对方案的安全性做了详细分析。

1 预备知识

1.1 前向安全签名的概念

前向安全签名的概念在文献[7]中已有详细说明,这里仅给出其形式化定义。

定义 若存在一个单向签名密钥更新算法 $KeyUd$,使得签名人可以在第 i 时间段将签名密钥由 σ_{i-1} 更新为 $\sigma_i = KeyUd(\sigma_{i-1})$,并在不同的时间段内使用不同的签名密钥 σ_i 生成签名 $Sign(\sigma_i, m)$(m 是消息),而任何验证人都可以用固定的公钥 Y 及时间段的编号 i 验证等式 $Ver[Y, i, Sign(\sigma_i, m), m]$ 成立,则签名 $Sign(\sigma_i, m)$ 为一个前向安全数字签名。

1.2 双线性映射

令 G_1 为由 P 生成的阶为素数 q 的循环加法群,G_2 为具有相同阶 q 的循环乘法群,双线性对是指是满足下列性质的一个映射 $e: G_1 \times G_1 \rightarrow G_2$:

到稿日期:2008-05-05 本文受863国家高科技研究发展计划基金(301-1-3),国家自然科学基金(60403027)资助。

夏祥胜 博士生,讲师,主要研究方向为数字签名、现代密码学等,E-mail:xiaxiangsheng@126.com;洪 帆 博导,教授,主要研究方向为现代密码学、安全模型及访问控制等;耿永军 博士生,主要研究方向为密钥管理、数字签名等;崔国华 博导,教授,主要研究方向为现代密码学、密钥管理等。

1)双线性：$e(aP,bQ)=e(P,Q)^{ab}$，对所有的 $P,Q\in G_1$，所有的 $a,b\in Z_q$ 成立；

2) 非退化性：存在 $P,Q\in G_1$，使得 $e(P,Q)\neq 1$；

3) 可计算性：对任意的 $P,Q\in G_1$，存在一个有效算法计算 $e(P,Q)$。

G_1 中的离散对数问题是已知 $P,Q\in G_1$，求 $a\in Z_q$，使得 $Q=aP$。这是一个公开的困难问题。

根据文献[16]的介绍，当群 G_1 上 DDH 问题(判定性 Diffie-Hellman问题)是简单的，而 CDH 问题(计算性 Diffie-Hellman 问题)是困难的时，我们称群 G_1 为 GapDiffie-Hellman(简称 GDH)群。这样的群能在有限域上的超奇异椭圆曲线或超椭圆曲线上找到，而双线性对可由 Weil 对或 Tate 对获得。本文提出的方案是基于 GDH 群的。

2 基于双线性对的前向安全的代理签名方案

2.1 系统初始化

设 G_1 为由 P 生成的阶为 q 的循环加法群，G_2 为具有相同阶 q 的循环乘法群，$e:G_1\times G_1\to G_2$ 为 $G_1\times G_1$ 到 G_2 的双线性映射，其中 q 为安全的大素数，$H_1:\{0,1\}^*\to G_1$，$H_2:\{0,1\}^*\times G_2\to Z_q^*$ 是安全的单向 Hash 函数。系统公开$\{G_1,G_2,e,q,P,H_1,H_2\}$。$A$ 为原始签名人，随机选择 $x_A\in Z_{q-1}^*$ 为私钥，计算 $y_A=x_AP$ 作为公钥予以公开。B 为代理签名人，随机选择 $x_B\in Z_{q-1}^*$ 为私钥，计算 $y_B=x_BP$ 作为公钥予以公开。

2.2 代理授权过程

1) 原始签名人 A 选择时间周期 $1,2,\cdots,T$，并生成委任状 m_w(包括原始签名人 A 和代理签名人 B 的身份标识、代理期限、代理权限和代理范围等相关信息)，计算 $\overline{S}_0=x_AH_1(m_w)$，$A$ 将$(\overline{S}_0,m_w)$公开发送给代理签名人 B，并公开参数 T。

2) 代理人 B 验证式(1)：

$$e(P,\overline{S}_0)=e(y_A,H_1(m_w)) \tag{1}$$

若等式成立，则接受代理。记 $x_{B,0}=x_B$，计算 $S_0=\overline{S}_0+x_{B,0}H_1(m_w)$作为代理签名初始密钥，并公开 $Y=x_{B,0}^{2^{T+1}} \bmod (q-1)$。$Y$ 可以预先计算。

2.3 前向安全的代理签名产生过程

设待签消息为 m。前向安全的代理签名产生过程如下：

1) 密钥更新。本方案对代理签名人的私钥进行更新，在每个周期的开始，代理签名人 B 根据前一周期的私钥 $x_{B,j-1}$ 计算出本周期的私钥 $x_{B,j}=x_{B,j-1}^2 \bmod (q-1)$，并计算 $S_j=\overline{S}_0+x_{B,j}H_1(m_w)$。然后，代理签名人 B 将周期序号 $j-1$ 更新为 j，并删除前一个周期 $j-1$ 的 $x_{B,j-1}$ 和 S_{j-1}。

2) 代理签名。B 任意选取 $\alpha_j\in Z_{q-1}^*$，计算：

$$u=e(P,P)^{\alpha_j} \tag{2}$$

$$h=H_2(m||m_w||u||j) \tag{3}$$

$$V=hS_j+\alpha_jP \tag{4}$$

则前向安全的代理签名为$[j,(h,V,m,m_w)]$。

2.4 前向安全的代理签名的验证

当签名验证人收到$[j,(h,V,m,m_w)]$后，首先根据委任状 m_w 判断代理人的签名是否存在代理权滥用、延期代理等。若存在，则代理签名无效。否则，计算：

$$u'=e(V,P)e(H_1(m_w),y_A+Y^{2^{j-T-1}}P)^{-h} \tag{5}$$

验证式(6)

$$h=H_2(m||m_w||u'||j) \tag{6}$$

若式(6)成立，则代理签名有效，否则代理签名无效。

3 方案的正确性证明

定理 1 若式(1)成立，则 B 可以接受原始签名人 A 的授权并成为其合法代理人。

证明：因为

$$e(P,\overline{S}_0)=e(P,x_AH_1(m_w))=e(x_AP,H_1(m_w))$$
$$=e(y_A,H_1(m_w))$$

所以，若式(1)成立，则 B 可以接受原始签名人 A 的授权并成为其合法代理人。

定理 2 若式(6)成立，则前向安全的代理签名$[j,(h,V,m,m_w)]$是有效的。

证明：因为

$$u'=e(V,P)e(H_1(m_w),y_A+Y^{2^{j-T-1}}P)^{-h}$$

其中，$e(V,P)=e(hS_j+\alpha_jP,P)$

$$=e(hS_j,P)e(\alpha_jP,P)=e(S_j,P)^he(P,P)^{\alpha_j},$$

$$e(H_1(m_w),y_A+Y^{2^{j-T-1}}P)^{-h}$$

$$=[e(H_1(m_w),y_A)e(H_1(m_w),(x_{B,0}^{2^{T+1}})^{2^{j-T-1}}P)]^{-h}$$

$$=[e(H_1(m_w),x_AP)e(H_1(m_w),x_{B,0}^{2^j}P)]^{-h}$$

$$=[e(x_AH_1(m_w),P)e(H_1(m_w),x_{B,j}P)]^{-h}$$

$$=[e(\overline{S}_0,P)e(x_{B,j}H_1(m_w),P)]^{-h}$$

$$=e(\overline{S}_0+x_{B,j}H_1(m_w),P)^{-h}$$

$$=e(S_j,P)^{-h}$$

所以有

$$u'=e(V,P)e(H_1(m_w),y_A+Y^{2^{j-T-1}}P)^{-h}$$
$$=e(S_j,P)^he(P,P)^{\alpha_j}e(S_j,P)^{-h}$$
$$=e(P,P)^{\alpha_j}=u$$

即有：

$$h=H_2(m||m_w||u||j)=H_2(m||m_w||u'||j)$$

因此，若式(6)成立，则前向安全的代理签名$[j,(h,V,m,m_w)]$是有效的。

4 方案的安全性分析

1) 方案具有前向安全性质

本方案的安全性基于以下假设：

强 RSA 假定：已知 n(n 为两个大素数的乘积，其分解未知)和 $c\in Z_n^*$，找出一个 $\alpha\in Z_n^*$ 满足 $\alpha^r\equiv c \bmod n$ 是一个非常困难的问题。

模合数平方剩余难题：设 $n=pq$ 其中 p 和 q 是两个不同的大素数，已知 n 和 $c\in Z_n^*$，则求 c 模合数 n 的平方根 $\alpha\in Z_n^*$ 满足 $\alpha^2\equiv c \bmod n$ 是一个非常困难的问题。

如果攻击者已获得代理签名人的第 j 周期的密钥 $x_{B,j}$，根据强 RSA 假定和模合数平方剩余难题，他无法通过 $x_{B,j}=x_{B,j-1}^2 \bmod (q-1)$ 求解 $x_{B,j-1}$，更无法求解 $x_{B,k}(k<j-1)$。因此，方案具有前向安全性质。

2)方案能抵抗伪造攻击

定理 3 攻击者若能获知第 j' 周期的代理签名私钥 $x_{B,j'}$，则可以构造有效的代理签名$[j',(h',V',m,m_w)]$。反之，在 $x_{B,j'}$ 未知的情况下，仅从代理签名方程式构造有效的代理签名是困难的。

证明：攻击者若获知 $x_{B,j'}$，则可以利用 $S_{j'}=\overline{S}_0+x_{B,j'}H_1(m_w)$ 计算出 $S_{j'}$，这里 $\overline{S}_0$ 是公开的。攻击者随机选择 $\alpha_{j'}\in Z_{q-1}^*$，计算：

$u'=e(P,P)^{\alpha_{j'}}$

$h'=H_2(m||m_w||u'||j')$

$V'=h'S_{j'}+\alpha_{j'}P$

则$[j',(h',V',m,m_w)]$能通过验证人的验证。因为验证人收到$[j',(h',V',m,m_w)]$后，首先计算(以下证明过程与定理2类似，此处从简)：

$\overline{u}'=e(V',P)e(H_1(m_w),y_A+Y^{2^{j'-T-1}}P)^{-h'}$

其中，$e(V',P)=e(h'S_{j'}+\alpha_{j'}P,P)$

$=e(h'S_{j'},P)e(\alpha_{j'}P,P)=e(S_{j'},P)^{h'}e(P,P)^{\alpha_{j'}}$，

$e(H_1(m_w),y_A+Y^{2^{j'-T-1}}P)^{-h'}$

$=[e(\overline{S}_0,P)e(x_{B,j'}H_1(m_w),P)]^{-h'}$

$=e(\overline{S}_0+x_{B,j'}H_1(m_w),P)^{-h'}$

$=e(S_{j'},P)^{-h'}$

所以有

$\overline{u}'=e(S_{j'},P)^{h'}e(P,P)^{\alpha_{j'}}e(S_{j'},P)^{-h'}$

$=e(P,P)^{\alpha_{j'}}=u'$

即有

$h'=H_2(m||m_w||u'||j')=H_2(m||m_w||\overline{u}'||j')$，因此式(6)成立，则$[j',(h',V',m,m_w)]$是有效的前向安全的代理签名。

另一方面，攻击者若不知 $x_{B,j'}$，则试图利用 $S_{j'}=\overline{S}_0+x_{B,j'}H_1(m_w)$ 计算不出 $S_{j'}$。他只能伪造一个 $S'_{j'}$，重新计算 $V'=h'S'_{j'}+\alpha_{j'}P$，则$[j',(h',V',m,m_w)]$不能通过验证人的验证。理由是(具体过程与上述类似，此处从简)：

$\overline{u}'=e(V',P)e(H_1(m_w),y_A+Y^{2^{j'-T-1}}P)^{-h'}$

其中，$e(V',P)=e(S'_{j'},P)^{h'}e(P,P)^{\alpha_{j'}}$，

$e(H_1(m_w),y_A+Y^{2^{j'-T-1}}P)^{-h'}$

$=[e(\overline{S}_0,P)e(x_{B,j'}H_1(m_w),P)]^{-h'}$

$=e(\overline{S}_0+x_{B,j'}H_1(m_w),P)^{-h'}$

$=e(S_{j'},P)^{-h'}$

注意 $S'_{j'}\neq S_{j'}$，所以有

$\overline{u}'=e(S'_{j'},P)^{h'}e(P,P)^{\alpha_{j'}}e(S_{j'},P)^{-h'}$

即有 $\overline{u}'\neq u'$，$h'=H_2(m||m_w||u'||j')\neq H_2(m||m_w||\overline{u}'||j')$，因此式(6)不成立，则$[j',(h',V',m,m_w)]$不是有效的前向安全的代理签名。定理3的结论成立。

定理3说明，在当前周期 j 的代理签名私钥 $x_{B,j}$ 泄露的情况下，周期 j 的代理签名是可以伪造的。根据强 RSA 假定，由当前周期 j 的 $x_{B,j}$ 求不出第 $t(1\leqslant t\leqslant j\leqslant T)$ 周期的 $x_{B,t}$，由定理3的结论可知，第 j 周期之前的代理签名是安全的，这也刚好体现了方案的前向安全性。定理3的结论也说明在代理人的私钥未知的情况下，方案能够抵抗伪造攻击。

当代理签名人当前周期 j 的代理秘钥 S_j 泄露时，攻击者试图通过 $S_j=\overline{S}_0+x_{B,j}H_1(m_w)$ 求出 $x_{B,j}$，将面临解决离散对数问题。因此，当代理签名人当前周期 j 的代理秘钥 S_j 泄露时，方案仍能够抵抗伪造攻击。

综上所述，攻击者想攻击成功，只有两种方法可供选择：

其一，构造代理签名方程(2)、(3)、(4)，以通过验证式(6)的验证。他必须知道或伪造当前周期 j 的代理签名私钥 $x_{B,j}$，尽管 $x_{B,j}=x_{B,0}^{2^j} \bmod (q-1)$，但 $x_{B,0}$ 已删除，无法求出 $x_{B,j}$。又由 $x_{B,0}=x_B$，攻击者想从代理签名人的公钥 y_B 求解 x_B(x_B 已删除)，将面临解决离散对数问题。他想通过公布的 $Y=x_{B,0}^{2^{T+1}} \bmod (q-1)$ 求出 $x_{B,0}$，也将面临求解离散对数难题。攻击者不知道代理人当前周期 j 的签名密钥 S_j，由 $S_j=\overline{S}_0+x_{B,j}H_1(m_w)$ 解出 $x_{B,j}$ 根本不可能。即便知道 S_j 求出 $x_{B,j}$，也将面临解决离散对数问题。上述分析表明，在不知 $x_{B,j}$ 的情况下，他想从代理签名方程入手伪造参数通过验证式(6)的验证是徒劳的。

其二，他就只有通过已知的验证式(6)来伪造相关代理签名参数。假定他已知(j,m,m_w,h)，他想通过式(3)$h=H_2(m||m_w||u||j)$求出 u，将面临解决单向散列函数求反问题。通过验证式 $h=H_2(m||m_w||u'||j)$，其中 $u'=e(V,P)e(H_1(m_w),y_A+Y^{2^{j-T-1}}P)^{-h}$ 求出 V，也将面临解决单向散列函数求反问题和解计算 Diffie-Hellman 困难问题。假定他已知(j,m,m_w,u)，则尽管可以通过式(3)$h=H_2(m||m_w||u||j)$求出 h，但他试图通过 $u=u'=e(V,P)e(H_1(m_w),y_A+Y^{2^{j-T-1}}P)^{-h}$ 求出 V，同样也将面临解决单向散列函数求反问题和解计算 Diffie-Hellman 难问题。因此，方案能抵抗伪造攻击。

3) 方案能够抵抗外部攻击

攻击者想从代理签名人的公钥 y_B 求解 x_B，将面临解决离散对数问题。他想通过公布的 $Y=x_{B,0}^{2^{T+1}} \bmod (q-1)$ 求出 $x_{B,0}$，也将面临求解离散对数难题。因此，他无法伪造代理签名。委任状 m_w 包括原始签名人 A 和代理签名人 B 的身份标识，攻击者无法伪造原始签名人对 B 授权而通过式(1)。因此，方案能够抵抗外部攻击。

4) 方案能实现签名权和代理签名权的有效分离

签名验证人在验证签名时必须同时使用原始签名人的公钥和代理签名人公开的验证公钥，使签名权和代理签名权实现了有效的分离。

5) 方案满足强代理签名的性质

根据以上的分析，只有代理签名人才可以生成有效的代理签名，任何人(包括原始签名人)都不能伪造代理签名。因此，方案满足强代理签名的可区分性、代理签名的不可抵赖性、可验证性、代理签名是得到原始签名人同意并授权的等安全性质。

6) 方案能够避免代理签名权的滥用

委任状 m_w 包括原始签名人 A 和代理签名人 B 的身份标识、代理期限、代理权限和代理范围等相关信息，并且是公开传送的，代理签名人不可能修改委任状 m_w，也就不能签署原始签名者未授权的消息，不能转让代理权，不能延期代理或永久代理等。

7) 方案简单、安全、方便、实用

本方案不需用秘密方式传送$(\overline{S}_0,m_w)$，代理签名人 B 可以通过原始签名人 A 公开的一些参数来验证授权的合法性。因此，本方案简单、安全、方便、实用。

结束语 本文给出了一个基于双线性对的代理签名方案，并引入了前向安全特性，有效地减少了由于代理密钥泄露而给系统造成的损失。详细分析了方案的安全性，指出方案在强 RSA 假定、模合数平方剩余难题、计算 Diffie-Hellman

困难问题等安全假设下是安全的。方案是基于双线性签名体制构造的，且不需用秘密方式传送授权信息，因此，具有签字短、安全、高效、实用等优点。

参 考 文 献

[1] Mambo M, Usuda K, Okamoto E. Proxy signature: delegation of the power to sign messages[J]. IEICE Trans Fundamentals, 1996, 79(9): 1338-1354

[2] Mambo M, Usuda K, Okamoto E. Proxy signature for delegation signing operation[A]// Proc. 3rd ACM Conference on Computer and Communications Security[C]. New Delhi: ACM Press, 1996: 48-57

[3] Zhang F G, Safavi-Naini R, Lin C Y. New proxy signature, proxy blind signature and proxy ring signature schemes from bilinear pairings. 2003. http://eprint.iacr.org/2003/104

[4] Yi L J, Bai G Q, Xiao G Z. Proxy multi-signature scheme: a new type of proxy signature scheme[J]. Electronics Letters, 2000, 36(6): 527-528

[5] Hsu C L, Wu T C. New nonrepudiable threshold proxy signature with known signers[J]. Journal of Systems and software, 2001, (58): 119-124

[6] Anderson R. Invited lecture// Proceedings of the 4th ACM Conference on Computer and Communications Security. Zurich, Switerland, 1997: 1-7

[7] 王晓明，陈火炎，符方伟. 前向安全的代理签名方案[J]. 通信学报，2005，26(11)：38-42

[8] 王晓明，符方伟，张震. 前向安全的多重数字签名方案[J]. 计算机学报，2004，27(9)：1177-1181

[9] 张晓敏，张建中. 一个改进的前向安全的代理签名方案[J]. 计算机工程，2007，33(21)：140-141

[10] Canetti R, Halevi S, Katz J. A Forward-secure signature public-key encryption scheme G// Advances in Cryptology-Eurocrypt'03[C]. LNCS2656. Berlin: Springer-Verlag, 2003: 255-271

[11] Bellare M, Miner S. A forward-secure digital signature scheme// Crypto'99. LNCE 1666. Berlin: Springer-Verlag, 1999: 431-448

[12] Kozlov A, Reyzin L. Forward-secure signature with fast key update // Proceedings of Security in Communication Network. Amalf, Italy, 2002: 241-256

[13] 冯华熹，冯登国. 一个基于双线性映射的前向安全门限签名方案[J]. 计算机研究与发展，2007，44(4)：574-580

[14] Hess F. Efficient identity based signature schemes based on pairings// Proceedings of selected Areas in Cryptography 2002. Newfoundland, Canada, 2002: 310-324

[15] Zhang F, Safavi-Naini R, Susilo W. An efficient signature scheme from bilinear pairings and its application // PKC'04. LNCS2947. Berlin: Springer-Verlag, 2004: 277-290

[16] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing // Proceedings of Advances in Cryptology-Asia Crypt 2001. LNCS2248. Berlin: Springer-Verlag, 2001: 514-532

(上接第 55 页)

界普及这些概念发生若干作用[10]。”

维纳是谦虚的，无意于争夺现代电子计算机发明的某些优先权，然而计算机学界与科技史界不应忘记，控制论创立者维纳曾是探索计算机设计原理的伟大先行者与创造者。

3 计算思维：交叉创新的发展路径

计算思维作为三大科学思维方式之一，如何开拓创新并实际运用，是关系到科技工作者的创新能力、计算机事业的发展前景乃至国家综合实力竞争的重大战略课题。

钱学森虽未提出过计算思维的概念和研究方法，但是却对一般思维的研究方法和发展思路提出过原则性的见解：1. 微观的结构方法；2. 宏观的功能方法；3. 形象思维是当前研究思维科学的突破口；4. 同人工智能和智能计算机的研究相结合；5. 与系统科学相结合[4]。计算思维属于思维科学的一个专门领域，钱学森关于一般思维科学的发展思路无疑也适用于推进计算思维的研究。

以笔者之见，除此之外，还应该强调学科交叉是计算思维创新的一条根本路径。计算思维的研究工作涉及基础科学、技术科学与工程技术三大科学层次，任一层次的相关成果，尤其是创新成果，都有可能促进计算思维的创新。

计算思维重大创新的历史经验告诉我们，似乎应特别重视基础科学与计算机之间的交叉互动。华罗庚作出的最后一个重大创新成果是与王元的合作成果——世界数学界称之为“华-王方法”。这一方法即是华罗庚的数论思想与计算机模拟相结合的方法。华罗庚与王元运用这一方法利用中国第一台电子管电子计算机的计算，解决了用纯数学的逻辑推导方法无法解决的高维数值积分问题[13]。而冯康创立的有限元法、哈密顿辛几何算法是中国计算机研究工作领先世界的两大成果，这两个算法的创新则是经典物理学原理与计算机方法相结合的产物。此外，中国还有吴文俊创立的“吴方法”，这一蜚声国际数学界的机证定理算法，则是吴文俊的数学机械化思想、多项式方程计算方法与计算机方法相结合的产物。由此可见，学科交叉是计算思维创新的重要途径。有抱负有能力的年轻一代科技工作者，尤其是计算机工作者，应该从中国计算科学创新大师身上获得攀登科学顶峰的深刻启示：深广独特的知识结构，纵横交叉的创新思路，终生不倦的探索精神。

参 考 文 献

[1] 董荣胜. 计算机科学与技术方法论[M]. 北京：人民邮电出版社，2002

[2] 董荣胜. 计算机科学导论——思想与方法[M]. 北京：高等教育出版社，2007

[3] 恩格斯. 自然辩证法[M]. 北京：人民出版社，1971：27

[4] 北京大学现代科学与哲学研究中心. 钱学森与现代科学技术[M]. 北京：人民出版社，2001：157

[5] 石钟慈. 第三种科学方法——计算机时代的科学计算[M]. 北京：清华大学出版社，2000：11

[6] 王文华. 钱学森学术思想[M]. 成都：四川科技出版社，2007：374

[7] 胡作玄，石赫. 吴文俊之路[M]. 上海：上海科技出版社，2002：130-133

[8] 康德. 未来形而上学导论[M]. 北京：商务印书馆，1978：38，57

[9] 李佩珊，许良英. 20 世纪科学技术简史[M]. 北京：科学出版社，1999：362

[10] 冯端. 零篇集存[M]. 南京：南京大学出版社，2003：506

[11] 陈厚云，王行刚. 计算机发展简史[M]. 北京：科学出版社，1985：35

[12] N·维纳. 控制论[M]. 北京：科学出版社，1985：3-4

[13] 王元. 华罗庚[M]. 北京：开明出版社，1994：247-251