



基于 PACDP 的全同态加密方案的一种攻击方法^{*}

王 政^{1,2}, 丁 勇^{1,2}, 李新国³, 柳 毅⁴

- (1. 桂林电子科技大学数学与计算科学学院 桂林 541004;
2. 西安电子科技大学综合业务网理论及关键技术国家重点实验室 西安 710126;
3. 深圳数字电视国家工程实验室股份有限公司 深圳 518057;
4. 广东工业大学计算机科学学院 广州 510006)

摘 要:针对汤等人设计的整数上具有更小公钥尺寸的全同态加密方案,研究安全性基于整数上部分近似公因子问题(PACDP)的全同态加密方案的攻击方法。通过对公钥噪声区间进行适当的分割,结合快速多项式多点求值,再利用 GCD 算法得到私钥,从而成功攻击安全性基于 PACDP 的全同态加密方案。

关键词:全同态加密;安全性;PACDP;快速多项式多点求值

doi: 10.3969/j.issn.1000-0801.2013.03.016

A Method to Attack the FHE Schemes Based on the Hardness of PACDP

Wang Zheng^{1,2}, Ding Yong^{1,2}, Li Xinguo³, Liu Yi⁴

- (1. School of Mathematics and Computational Science, Guilin University of Electronic Technology, Guilin 541004, China;
2. The State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710126, China;
3. Shenzhen Digital TV National Engineering Laboratory Co., Ltd., Shenzhen 518057, China;
4. School of Computer Science, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: For the FHE scheme designed by Tang et al, the security of the FHE schemes based on the hardness of a partially approximate integer common divisor problem (PACDP) was discussed. By dividing the interval of the noise of the public key, using the fast polynomial multipoint evaluation and GCD algorithm to get the secret key, the FHE schemes based on the hardness of PACDP were successfully crashed down.

Key words: fully homomorphic encryption, security, PACDP, fast polynomial multipoint evaluation

1 引言

1978 年 Rivest、Adleman 和 Dertouzos 提出“隐私同态”^[1]的思想,即希望在不解密密文的前提下,对密文进行任意复杂的操作。在此之后,出现了多种方案,但都不能实现任意

次计算。直到 2009 年, Gentry 提出了一个基于理想格的全同态加密方案^[2],并在参考文献[3]中给出了构造全同态加密方案的具体思路。2010 年, Van Dijk 等根据 Gentry 的构造思想,提出了基于整数上近似最大公因子问题的全同态加密方案^[4]。2011 年, Coron 等在参考文献[5]中用公钥的平方

^{*} 国家“863”项目基金资助项目(No.2012AA011705),国家自然科学基金资助项目(No. 60963024),广东省教育部产学研结合项目(No. 2012B091000060),广西无线宽带通信与信号处理重点实验室 2012 年开放基金资助项目,综合业务网理论及关键技术国家重点实验室 2012 年开放基金资助项目



形式代替原方案中的线性形式,将参考文献[4]方案中的公钥尺寸由 $\tilde{O}(\lambda^{10})$ 减小为 $\tilde{O}(\lambda^7)$,并结合参考文献[6]中的方法优化了解密电路。随后其又在参考文献[7]中用伪随机数发生器的方式将公钥的尺寸进一步缩小为 $\tilde{O}(\lambda^5)$,并结合参考文献[8]中的方法,使 Van Dijk 等的方案无需自举就能够实现全同态。参考文献[9]对参考文献[4]中方案的公钥进行了更大的简化,将方案的安全性归约为整数上部分近似公因子问题(PACDP),并引入了参考文献[10]中的“可忽略概率解密错误”的思想。参考文献[11]使用格归约攻击方法直接获取密文中的明文比特,破解了汤等人的全同态加密方案。

参考文献[12]通过对区间 $[0, 2^p]$ 进行适当的分割,结合快速多项式多点求值,给出了能够更快解决 PACDP 的算法。但该方案只适合噪声 r 在 $[0, 2^p]$ 上的 PACDP,并不满足安全性基于 PACDP 的全同态加密方案中公钥噪声 r 的范围为 $(-2^p, 2^p)$ 的情况,因此不能够直接用来攻击此类全同态加密方案。本文把参考文献[12]中 r 的取值范围 $[0, 2^p]$ 由扩大为 $(-2^p, 2^p)$,使其能够用来解决 r 在 $(-2^p, 2^p)$ 上的 PACDP,且满足安全性基于 PACDP 的同态加密方案中公钥噪声 r 的范围。通过将此噪声范围进行对称分割,利用快速多项式多点求值求出每一个分割区间中所有的 $(x_1-i)(x_1+i)$ 的乘积,在得到的所有乘积中必有一个是 p 的倍数,因此能够通过 GCD 运算求出 x_0 与这些乘积之间的最大公因数,即私钥 p 。在汤等的方案中,其安全性是基于 PACDP 的,本文将针对该方案研究能够成功攻击安全性基于 PACDP 的全同态加密方案的方法。

2 汤等的同态加密方案

2.1 相关定义

定义 1 (符号 $\tilde{O}$) $f(n)=\tilde{O}(g(n))$ 是指存在常数 $N, c \in N$, 使得当 $n \geq N$ 时, $f(n)=O(g(n)(\lg g(n))^c)$ 成立。

对于一个实数 z 和一个整数 p , 用 $z \bmod p$ 表示 z 除以 p 的余数,且 $z \bmod p \in (-p/2, p/2)$ 。本文中用 $z \bmod p$ 表示模运算,包括多项式的模运算也取该范围。

文中的对数运算都是以 2 为底的。

定义 2 (部分近似公因子问题^[13]) 设 p 是大素数,给定两个整数 x_0, x_1 , 其中 $x_0=pq_0, x_1=pq_1+r, |r|<p, q_i \in Z(i=0, 1)$ 根据 x_0, x_1 求素数 P 。

2.2 Somewhat 同态加密方案

本文的方法是对公钥进行攻击,因此既适合 Somewhat

同态加密方案^[9]也适合全同态加密方案。本文将选择 Somewhat 同态加密方案来研究,因为其是全同态加密方案的基础组成部分,如果攻破了 Somewhat 同态加密方案,则基于 Somewhat 同态加密方案构造的全同态加密方案也就攻破了。因此在本文中只引用了参考文献[9]中的 Somewhat 同态加密方案,而略去全同态加密方案。为了方便讨论,将文献中方案的密钥生成算法和加密算法做了适当的改变,但不会影响方案的正确性和安全性。

参数选取: $p=\lambda, p'=2\lambda, \eta=\tilde{O}(\lambda^2), \theta=\lambda^4, r=\tilde{O}(\lambda^5), \lambda$ 为安全参数。

密钥生成算法: 随机选择 η bit 的奇素数 p 和 θ bit 的奇素数 q_0 , 令 $x_0=pq_0$ 。再选取两个随机整数 $q_1 \in [0, 2^p/p], r \in (-2^p, 2^p)$, 计算 $x_1=pq_1+r$, 输出公钥 $pk=(x_0, x_1)$, 私钥 $sk=p$ 。

加密算法: 给定消息 $m \in \{0, 1\}$ 和公钥 $pk=(x_0, x_1)$, 选取两个随机整数 $r_1 \in (-2^{p'}, 2^{p'})$ 和 $r_2 \in (-2^p, 2^p)$, 计算并输出密文 $(c=m+2r_1+2r_2x_1) \bmod x_0$ 。

解密算法: 根据给定的密文 c 和私钥 $sk=p$, 计算并输出明文 $m' \leftarrow (c \bmod p) \bmod 2$ 。

选取适当的参数,不难验证上述方案的解密正确性以及密文的同态加和同态乘的性质。该方案的安全性是基于 PACDP 的,安全性证明详见参考文献[9]。

3 攻击算法

设两个整数 $x_0=pq_0, x_1=pq_1+r, -2^p < r < 2^p, x_0 > x_1$ 。当 2^p 较小时,求 p 的最好方法是 GCD 穷举搜索,即尝试 r 在区间 $(-2^p, 2^p)$ 中每一个可能的整数值,通过求出每一个 $\gcd(x_0, x_1-i)$ 进而得到 p 。若 p 是 r 的比特长度,则用这种方法需要 2^{p+1} 次 GCD 运算。本文将通过对参考文献[12]中的方法进行适当的改进,使得当 $r \in (-2^p, 2^p)$ 时,只需要进行 $\tilde{O}(\sqrt{2^p})$ 次运算。

因为 $r \in (-2^p, 2^p)$, 故在区间 $(-2^p, 2^p)$ 中,必存在一个整数值 i , 使得 x_1-i 是 p 的整数倍,因此所有的 $x_1-i, i \in (-2^p, 2^p)$ 之积也必为 p 的整数倍,可进一步通过求这个积与 x_0 的最大公因子得到 p , 即:

$$p = \gcd(x_0, \prod_{i=-2^p+1}^{2^p-1} (x_1-i) \bmod x_0) \quad (1)$$

通过式(1)求 p , 将用 $2^{p+1}-2$ 次模乘运算(每个数均为 γ bit) 和一次 GCD 运算取代穷举搜索中的 2^{p+1} 次 GCD 运算(每个数均为 γ bit)。在参考文献[5]中给出了两个 γ 比特整数的 GCD 运算和模乘运算的运算时间,见表 1。

表1 两个 γ 比特整数的 GCD 运算和模乘运算所用时间的比较

γ	2^{21}	2^{22}	2^{23}	2^{24}	2^{25}
GCD 运算时间(s)	2.7	6.7	16.4	39.2	89.9
模乘运算时间(s)	0.5	1.2	2.8	6.7	15.4

由表1可知,用式(1)能够比 GCD 穷举搜索更快地求出 p 。

在参考文献[12]中,只给出了当 $r \in [0, 2^p]$ 时的情形,本文将 r 的取值范围扩大为 $(-2^p, 2^p)$,以满足全同态加密算法的要求,为此将式(1)稍做改变,得:

$$p = \gcd(x_0, \prod_{i=-2^{p'}+1}^{2^{p'}-1} x_1(x_1 - i) \pmod{x_0}) \quad (2)$$

令 $p' = \lfloor p/2 \rfloor$, 则有 $p' + (p \bmod 2) = p - p'$ 。定义如下次数为 $2^{p'+1}$ 的多项式:

$$f(x) = \prod_{i=0}^{2^{p'}-1} (x_1 - (x + i))(x_1 + (x + i)) \pmod{x_0} \quad (3)$$

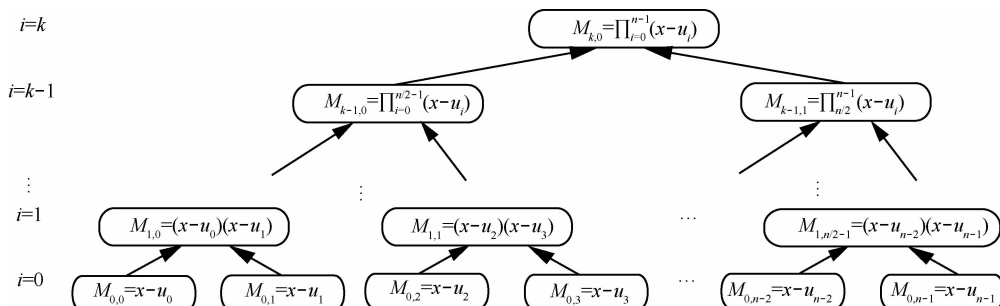
则有:

$$\begin{aligned} f(t \cdot 2^{p'}) &= \prod_{i=0}^{2^{p'}-1} (x_1 - (t \cdot 2^{p'} + i))(x_1 + (t \cdot 2^{p'} + i)) \\ &= \prod_{i=t \cdot 2^{p'}}^{(t+1) \cdot 2^{p'}-1} (x_1 - i)(x_1 + i), \quad 0 \leq t \leq 2^{p-p'} - 1 \end{aligned} \quad (4)$$

进一步能够得到:

$$\begin{aligned} \prod_{t=0}^{2^{p-p'}-1} f(t \cdot 2^{p'}) &= f(0) \cdots f(t \cdot 2^{p'}) \cdots f((2^{p-p'} - 1) \cdot 2^{p'}) \\ &= \prod_{i=0}^{2^{p'}-1} (x_1 - i)(x_1 + i) \cdots \prod_{i=t \cdot 2^{p'}}^{(t+1) \cdot 2^{p'}-1} (x_1 - i) \\ &\quad (x_1 + i) \cdots \prod_{i=2^{p'}-2^{p'}}^{2^{p'}-1} (x_1 - i)(x_1 + i) \\ &= \prod_{i=0}^{2^{p'}-1} (x_1 - i)(x_1 + i) \end{aligned} \quad (5)$$

根据上述过程,可以将式(2)写为:


 图1 在点 $u_0, \dots, u_{n-1}$ 处的多项式乘积树 $M = [M_{0,0}, \dots, M_{k,0}]$

$$p = \gcd(x_0, \prod_{t=0}^{2^{p-p'}-1} f(t \cdot 2^{p'}) \pmod{x_0}) \quad (6)$$

接下来将通过多项式多点求值求出式(6)中每一个 $f(t \cdot 2^{p'})$ 的值,并对这些值求积,再利用式(6)通过 GCD 运算求出私钥 p 。

定义3 (多项式多点求值) 令 $n = 2^k (k \in \mathbb{N})$, 多项式 $f \in \mathbb{Z}[x]$, f 的次数小于 n , 且点 $u_0, \dots, u_{n-1} \in \mathbb{Z}$, 计算 $f(u_0, t=0, \dots, n-1)$ 。

算法1 输入 $n = 2^{p-p'}$ 个单项式 $m_t = x - u_t (t=0, \dots, n-1)$, 在本文中点 u_t 的值分别取 $u_t = t \cdot 2^{p'} (t=0, \dots, n-1)$, 输出每一个多项式 $M_{i,j}$, 其中 $M_{i,j} = m_{j \cdot 2^i} \cdots m_{j \cdot 2^i + (2^i - 1)} = \prod_{i=0}^{2^i-1} m_{j \cdot 2^i + i}, 0 \leq i \leq k = \lfloor \log n \rfloor, 0 \leq j < 2^{k-i}$ (如图1所示)。

令 $M_{0,j} = m_j, M_{k,0} = \prod_{j=0}^{n-1} m_j$, 则多项式 $M_{k,0}$ 的次数为 $2^{p-p'}$ 。

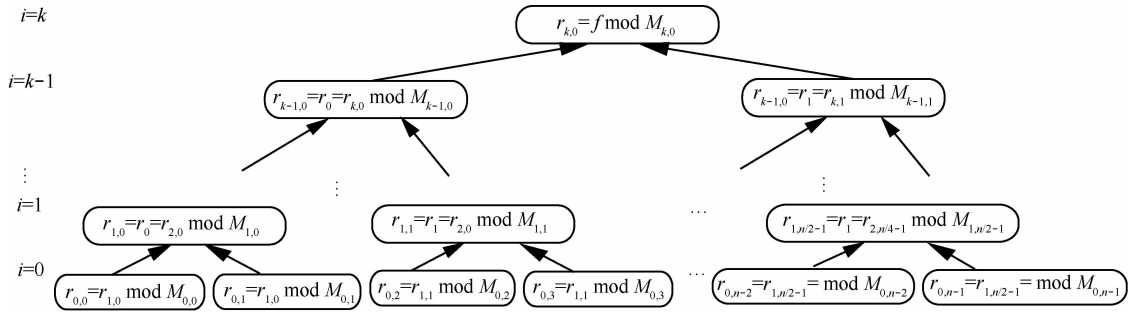
在算法1中的每一个多项式 $M_{i,j}$ 都是多项式乘积树中 $M_{k,0}$ 的 2^i 个单因子 $M_{0,j}$ 的乘积,且对每一个 i, j 都有 $M_{i+1,j} = M_{i,2j} \cdot M_{i,2j+1}$ 则通过该关系式可以递推求出每一个多项式 $M_{i,j}$ 。令多项式 $g(x) = f(x) \pmod{M_{k,0}}$, 则 $g(x)$ 的次数低于 $2^{p-p'}$ 。

算法2 输入上述多项式 $g(x), n$ 个点 $0, 2^{p'}, \dots, (n-1) \cdot 2^{p'}, n = 2^{p-p'}$, 算法1中求出的每一个多项式 $M_{i,j}$ 。分别输出多项式 $g(x)$ 在这些点的值 $g(0), g(2^{p'}), \dots, g((n-1) \cdot 2^{p'})$ 。

在图2中,设模去多项式 $M_{i,j}$ 的剩余为 $r_{i,j}(x)$, 用 $r_{i,j}(x)$ 模 $M_{i,j}$ 的左子节点的剩余为 $r_0(x)$, 即 $r_{i-1,2j}(x)$; 用 $r_{i,j}(x)$ 模 $M_{i,j}$ 的右子节点的剩余为 $r_1(x)$, 即 $r_{i-1,2j+1}(x)$ 。依此类推,直到求出模 $M_{0,j}$ 的剩余,记为 $r_{0,j}(x)$ 。令 $g(x) \pmod{M_{k-1,0}, M_{k-1,1}}$ 的商分别为 $q_0(x), q_1(x)$, 则有:

$$g(u_t) = \begin{cases} q_0(u_t) M_{k-1,0}(u_t) + r_0(u_t) = r_0(u_t), & 0 \leq t < \frac{n}{2} \\ q_1(u_t) M_{k-1,1}(u_t) + r_1(u_t) = r_1(u_t), & \frac{n}{2} \leq t < n \end{cases} \quad (7)$$

上述产生的每一个 $r_{i,j}(x)$ 都满足式(7),可以求出每一

图2 在点 $u_0, \dots, u_{n-1}$ 处的值 $M=\{M_{0,0}, \dots, M_{k,0}\}$

个 $r_{0,j}(u_j)$ 的值,且有 $g(u_j)=r_{0,j}(u_j)$ 。因为 $g(x)=f(x) \bmod M_{k,0}$, 则存在多项式 $q(x)$ 使得 $f(x)=q(x)M_{k,0}+g(x)$, 又 $M_{k,0}=\prod_{t=0}^{n-1} (x-u_t)$, 所以 $f(u_j)=g(u_j)=r_{0,j}(u_j)$, 故求出了 f 在每一个点的值,从而可进一步求出式(6)中的 $\prod_{t=0}^{2^{p-p'}-1} f(u_t)$ 。

若存在:

$$r \in (-(j+1) \cdot 2^{p'}, -j \cdot 2^{p'}) \cup [j \cdot 2^{p'}, (j+1) \cdot 2^{p'}) \quad (8)$$

则在该区间中必存在一个整数 i , 使得 $(x_1-i)(x_1+i)$ 为 p

的整数倍, 故有 $\prod_{i=j \cdot 2^{p'}}^{(j+1) \cdot 2^{p'}-1} (x_1-i)(x_1+i) \equiv 0 \pmod{p}$ 。因为

$$f(u_t)=f(t \cdot 2^{p'})=\prod_{i=t \cdot 2^{p'}}^{(t+1) \cdot 2^{p'}-1} (x_1-i)(x_1+i), \quad 0 \leq t \leq n-1, \text{ 所}$$

以 $f(u_t)$ 也必为 p 的整数倍。故在整个区间 $(-2^p, 2^p)=[0, 2^{p'}) \cup (-2^p, 0] \cup \dots \cup [2^p-2^{p'}, 2^p) \cup (-2^p, -2^p+2^{p'}]$ 上, 一定满足

$$\prod_{t=0}^{n-1} f(u_t) \text{ 为 } p \text{ 的整数倍, 因此能通过式(6)利用 GCD 运算}$$

把私钥 p 求出来, 从而成功破解了该同态加密方案。

要求 $f(0), f(2^{p'}), \dots, f((2^{p-p'}-1) \cdot 2^{p'})$ 这些值, 如果用余数定理将需要 $O(n^2)$ 次运算, 而结合算法 1 和算法 2, 则只需要 $O(M(n) \lg n)$ 次运算, 其中 $M(n)$ 表示两个次数低于 n 的单变量多项式乘积所需的运算次数, 最大为 $63.427 \cdot n \cdot \lg n \cdot \lg \lg n + O(n \cdot \lg n)$ 。再加上 $2^{p-p'}-1$ 次模乘运算和一次 GCD 运算就可以求得私钥 p 。在本文中点 u_k 的个数与参考文献[12]中点的个数相等, 因此用该方法只需要 $\tilde{O}(2^{p'})=\tilde{O}(\sqrt{2^p})$ 次运算, 但 r 的范围却扩大为 $(-2^p, 2^p)$ 。由于算法中多项式的计算都是模乘运算, 且模乘运算比 GCD 运算要快很多。

在参考文献[12]中, 给出了当 $r \in [0, 2^p)$ 时穷举搜索法和新方法所需时间的比较, 部分数据见表 2。

表2 GCD 穷举搜索与参考文献[12]中新方法所需时间的比较

γ	1.6×10^5	0.86×10^6	4.2×10^5
ρ	16	24	32
GCD 穷举搜索所需要时间	40 min	96 天	623 年
参考文献[12]中新方案所需时间	1.6 min	7.1 h	190 天

从表 2 中可以看出, 参考文献[12]中的新方法比穷举搜索法要快很多。特别地, 当 ρ 较小时, 更能够体验新方法的优越性。本文主要是对参考文献[12]中 r 的范围进行了扩展, 并在方法的设计方面做了相应的改进, 在原理方面与文献中方法保持一致, 主要运算量都来自于多项式多点求值, 故本文中的方法与文献中的方法在运算量和运算速度上具有相同的特性。但参考文献[12]中的方法只能解决 $r \in [0, 2^p)$ 上的 PACDP, 不能够直接用来攻击安全性基于 PACDP 的全同态加密方案, 而本文改进后的方法将能够解决 $r \in (-2^p, 2^p)$ 上的 PACDP, 从而能够成功地攻击安全性基于 PACDP 的全同态加密方案。

4 结束语

本文针对汤等人设计的整数上具有更小公钥尺寸的全同态加密方案, 研究安全性基于 PACDP 的全同态加密方案的攻击方法。对于安全性基于 PACDP 的全同态加密方案, 当噪声的比特长度 ρ 较小时, 通过对公钥噪声区间进行适当的分割, 结合多项式多点求值, 再利用 GCD 算法得到私钥 p , 从而能够成功攻击安全性基于 PACDP 的全同态加密方案。

参考文献

- 1 Ronald L R, Len A, Michael L D. On data banks and privacy homomorphisms. Foundations of Secure Computation, New York, 1978:169~180

- 2 Gentry Craig. Fully homomorphic encryption using ideal lattices. STOC 2009, Bethesda, Maryland, USA, 2009:169~178
- 3 Gentry Craig. A fully homomorphic encryption scheme. PhD Thesis, Stanford University. <http://crypto.stanford.edu/craig>, 2009
- 4 Van Dijk Marten, Gentry Craig, Halevi Shai, *et al.* Fully homomorphic encryption over the integers. EUROCRYPT 2010, LNCS, 2010: 24~43
- 5 Jean-Sebastien C, Avradip M, David N, *et al.* Fully homomorphic encryption over the integers with shorter public keys. P Rogaway (Ed), CRYPTO 2011, LNCS, Springer, 2011:487~504
- 6 Gentry Craig, Halevi Shai. Implementing gentry's fully-homomorphic encryption scheme. Paterson, KG (ed) EUROCRYPT 2011, LNCS, Springer, Heidelberg, 2011: 129~148
- 7 Jean-Sebastien C, David N, Mehdi T. Public Key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers. Cryptology ePrint Archive Report, 2011
- 8 Brakerski Zvika, Gentry Craig, Vaikuntanathan Vinod. Fully Homomorphic Encryption without Bootstrapping. Cryptology ePrint Archive Report, 2011
- 9 汤殿华,祝世雄,曹云飞. 一个较快速的整数上的全同态加密方案. 计算机工程与应用. <http://www.cnki.net/kcms/detail/11.2127.TP.20110804.1604.040.html>, 2011
- 10 Stehlé Damien, Steinfeld Ron. Faster fully homomorphic encryption. Asiacrypt 2010, LNCS, 2010: 377~394
- 11 古春生,景征骏,于志敏. 破解较快速的整数上的全同态加密方案. 计算机工程与应用. <http://www.cnki.net/kcms/detail/11.2127.TP.20120601.1456.003.html>, 2012
- 12 Chen Y M, Nguyen P Q. Faster Algorithms for Approximate Common Divisors Breaking Fully-Homomorphic-Encryption Challenges over the Integers. Cryptology ePrint Archive Report, 2011
- 13 Howgrave-Graham Nick. Approximate integer divisors. CaLC'01, Lecture Notes in Computer Science, Springer, 2001: 51~66

[作者简介]

王政,男,桂林电子科技大学硕士研究生,主要研究方向为全同态加密。

丁勇,男,博士,桂林电子科技大学教授,主要研究方向为密码学与信息安全。

李新国,男,博士,深圳数字电视国家工程实验室股份有限公司技术总监,主要研究方向为数字多媒体安全。

柳毅,男,博士,广东工业大学副教授,主要研究方向为密码学与网络安全。

(收稿日期:2012-12-25)

·简讯·

未来网络入选国家重大科技 基础设施建设中长期规划

近日,国务院正式发布《国家重大科技基础设施建设中长期规划(2012-2030年)》,其中,信息技术和未来网络实验设施分别被纳入总体部署的7大重点领域和“十二五”时期国家的建设重点。

规划明确了未来总体部署的7大重点领域,其中信息技术被纳入工程技术科学领域。规划提出,在信息技术方面,建设未来网络研究设施,解决未来网络和信息系统发展的科学技术问题,为未来网络技术发展提供试验验证支撑;适时启动新一代授时系统建设,支撑超精密时间频率技术开发,逐步形成高精度卫星授时系统和高精度地基授时系统共同发展的格局。

规划共提出了16项“十二五”时期的建设重点。其中,第8项为未来网络试验设施。规划明确指出,三网融合、云计算和物联网发展对现有互联网的可扩展性、安全性、移动性、能耗和服务质量都提出了巨大挑战,基于TCP/IP的互联网依靠增加带宽和渐进式改进已经无法满足未来发展的需求。为突破未来网络基础理论和支撑新一代互联网实验,建设未来网络试验设施,主要包括:原创性网络设备系统、资源监控管理系统,涵盖云计算服务、物联网应用、空间信息网络仿真、网络信息安全、高性能集成电路验证以及量子通信网络等开放式网络试验系统。该设施建成后,网络覆盖规模超过10个城市,支撑不少于128个异构网络并行实验,将为空间网络、光网络和量子网络研究提供必要的实验验证条件。

(来源:人民邮电报)