耦合双触发元胞自动机的加密技术研究*)

赵学龙　李千目　平　萍　刘凤玉

(南京理工大学计算机科学与技术学院　南京 210094)

摘　要　针对单向触发元胞自动机加密中误差传播的相似性问题，以及双向触发元胞自动机中密钥空间小的问题，提出了耦合双触发元胞自动机的加密技术，通过相互作用、相互影响的元胞自动机系统之间的共同演化，反向迭代完成数据加密，正向演化完成数据解密，达到解决密文相似性问题以及增加密钥的目的。分析结果表明，该算法可以抵抗蛮力攻击和已知明文、已知密文以及差分分析攻击，具有较高的安全性和很强的实用性。

关键词　耦合元胞自动机，双触发规则，密码学，加密算法

Application of Coupled Bi-directional Toggle Cellular Automata on Data Encryption

ZHAO Xue-Long　LI Qian-Mu　PING Ping　LIU Feng-Yu

(Department of Computer Science and Technology, Nanjing University of Science & Technology, Nanjing 210094)

Abstract　A cryptography system based on the coupled bi-directional toggle cellular automata is proposed to solve the similarity flaw in the toggle cellular automata and enlarge the key space in bidirectional toggle ones. The encryption and decryption of data is completed by the evolution of the mutual influence of the cellular automata. The analysis results show that the cryptosystem can resist brute attack and differential attack, and also has high security and strong practicability.

Keywords　Coupled cellular automata, Bi-directional toggle rules, Cryptography, Encryption algorithms

1　引言

随着网络信息数字化的发展，保证信息的安全传输、存储成为目前面临的重要问题，因此密码学研究在信息安全中起着重要的作用。大量数据的处理需要高速的密码算法。元胞自动机(CA)由于其具有规整、模块化以及内在的并行性，便于软件和硬件实现等特点，可以快速完成加密和解密，尤为适合在大量数据加密处理中的应用[1]。

Wolfram[2]首先提出元胞自动机在密码学中的应用后，很多学者都对元胞自动机在密码学中的应用做了深入的研究[3~6]。Gutowitz[7]提出利用元胞自动机的触发特性可以快速构造先导状态，只要把数据编码成初始状态，把元胞自动机动力系统作为密钥，反向演化实现加密，正向演化实现解密，即可完成动力系统对信息数据进行加解密的过程，实现了对称密码算法。Oliveira 等人[6]对 Gutowitz 方法进行了改进，提出采用双向的元胞自动机实现加密，解决了误差单向传播的问题。但是，由于双触发元胞自动机规则的数量要比单触发元胞自动机的规则少得多，导致密钥空间太小，难以满足安全性的要求，因而必须通过增加规则半径来增加密钥空间，而这又带来计算量的大大增加。

本文提出耦合双触发元胞自动机来完成加密和解密，保留了双触发元胞自动机加密中误差传播快的优点[9]，同时使在相同的规则半径下，密钥空间成倍增加，大大提升密码系统的抗攻击性能。仿真试验结果表明，这种方法不仅解决了密文相似性的问题，提高了密钥空间，还可以抵抗差分分析等攻击，从而提高密码系统的强度。

2　触发元胞自动机

元胞自动机是时间、空间和状态都离散的动力系统，最早由 von Neumann 提出，用于模拟复杂系统的自复制现象[8]。触发元胞自动机是一类特殊的元胞自动机，即当改变元胞自动机中的某个元胞的状态时，其演化的状态也随之改变，这个元胞自动机称为触发元胞自动机，引起元胞状态值改变的元胞称为触发元胞。触发元胞自动机演化过程的一般表达式为

$$1-s_i^{t+1}=f(s_{i-r}^t,\cdots,1-s_{i-j}^t,\cdots,s_{i+r}^t)-r\leqslant j\leqslant r\quad j\in Z \tag{1}$$

式中 s_i^t 是元胞 i 在 t 时刻的状态，r 为元胞自动机的规则半径，元胞 j 为触发元胞，Z 为整数集。式(1)表明，只要改变触发元胞的值，则整个元胞自动机的演化状态也随之改变。当 $j=r$ 时，即最左侧的元胞为触发元胞，公式(1)就表示左触发元胞自动机，即

$$1-s_i^{t+1}=f(1-s_{i-r}^t,\cdots,s_i^t,\cdots,s_{i+r}^t) \tag{2}$$

同理，当 $j=-r$ 时，公式(1)就表示右触发元胞自动机。

如果改变元胞自动机任何一端的元胞状态值，整个元胞自动机的演化状态都随之改变的元胞自动机，称为双触发元胞自动机，其一般表达式为

$$1-s_i^{t+1}=f(1-s_{i-r}^t,\cdots,s_i^t,\cdots,s_{i+r}^t)=f(s_{i-r}^t,\cdots,s_i^t,\cdots,1-s_{i+r}^t) \tag{3}$$

可以看出，双触发元胞自动机是左触发和右触发元胞自动机的交集，因而对于相同规则半径的元胞自动机来说，其规

*)国家自然科学基金(60273035)和北方工业公司基础应用项目(K1704060511)资助。**赵学龙**　讲师，主要研究领域为信息安全、元胞自动机、加密技术理论与算法设计等；**李千目**　讲师，主要研究方向为网络安全认证；**平　萍**　博士研究生，主要研究方向为加密算法研究；**刘凤玉**　教授，博士生导师，主要研究方向为信息安全技术。

则数量要大大减少。

3 耦合双触发元胞自动机

Gutowitz 提出的加密模型中使用的是单(左或右)触发规则作为密钥。把明文编码成初始状态,利用触发性质构造先导状态,反向迭代完成数据加密,正向演化完成数据解密。由于采用的是单触发元胞自动机,改变一位明文和改变一位密文的误差扩散都是单向的,攻击者通过寻找密文的相似性就可以获得明文的信息,从而降低密码系统的安全性。为了弥补这个缺陷,Oliveira 等人[6]采用双触发规则来弥补这个缺陷。但是,这种方法的问题在于密钥空间太小,但对于采用触发规则作为密钥的密码系统来说,密钥空间的大小在一定程度上决定了密码系统的安全性。要想获得相同的密钥空间,就必须增大规则半径,而这又大大增加了计算量。本文采用两个双触发元胞自动机进行耦合,就可以以较少的计算量达到增加密钥空间的目的。

3.1 耦合双触发元胞自动机的基本原理

耦合元胞自动机是指不同元胞自动机的状态演化互相影响,互相作用,共同决定 CA 系统的演化状态。考虑由两个简单元胞自动机 A,B 构成的耦合元胞自动机:

$$\begin{aligned} A&: s_{a,i}^{t+1}=f(s_{a,i-r}^{t},\cdots,s_{b,i}^{t},\cdots,s_{a,i+r}^{t})\\ B&: s_{b,i}^{t+1}=g(s_{b,i-r}^{t},\cdots,s_{a,i}^{t},\cdots,s_{b,i+r}^{t}) \end{aligned} \tag{4}$$

A 的元胞演化不仅与 A 的邻居状态有关,还和配对的 B 的元胞状态有关,B 的状态演化与配对的 A 的元胞状态也有关,这样就构成了一个耦合元胞自动机系统。如果只考虑左触发元胞自动机,则有

$$\begin{aligned} 1-s_{a,i}^{t+1}&=f(1-s_{a,i-r}^{t},\cdots,s_{b,i}^{t},\cdots,s_{a,i+r}^{t})\\ 1-s_{b,i}^{t+1}&=g(1-s_{b,i-r}^{t},\cdots,s_{a,i}^{t},\cdots,s_{b,i+r}^{t}) \end{aligned} \tag{5}$$

如果触发元胞自动机的规则是双向的,则构成耦合双触发元胞自动机:

$$\begin{aligned} 1-s_{a,i}^{t+1}&=f(1-s_{a,i-r}^{t},\cdots,s_{b,i}^{t},\cdots,s_{a,i+r}^{t})\\ &=f(s_{a,i-r}^{t},\cdots,s_{b,j}^{t},\cdots,1-s_{a,i+r}^{t})\\ 1-s_{b,i}^{t+1}&=g(1-s_{b,i-r}^{t},L,s_{a,i}^{t},\cdots,s_{b,i+r}^{t})\\ &=g(s_{b,i-r}^{t},\cdots,s_{a,i}^{t},\cdots,1-s_{b,i+r}^{t}) \end{aligned} \tag{6}$$

这样,两个元胞自动机通过状态之间的相互作用和共同演化,完成整个 CA 系统的演化,构成一个耦合双触发元胞自动机。如果单个触发元胞自动机的密钥空间是 k_s,则这种耦合触发元胞自动机的密钥空间为 $k_s\times k_s$。

3.2 双触发元胞自动机规则的构造

在元胞自动机的规则半径为 1、元胞状态为 2,且触发元胞位于邻域两侧的情况下,双触发条件的元胞自动机可以用下图来表示:

000	001	010	011	100	101	110	111
①	②	③	④	⑤	⑥	⑦	⑧

图中上面一行表示初等元胞自动机的 8 种状态组合,下面一行用数字来区分表示这些组合。(I)根据左触发的性质,⑤⑥⑦⑧的状态值分别对应①②③④的状态值取反。(IIII)根据右触发的性质,②④⑥⑧的状态值分别对应①③⑤⑦的状态值取反。因此,我们首先确定①和③的值,从而根据这两个值,唯一确定②和④的值,最后可唯一确定⑤⑥⑦⑧。①和③的状态组合共有 00、01、10 和 11 四种。例如当①和③取值为 00 时,可唯一确定的双触发规则是 01011010(二进制),用 Wolfram 的命名法则来表示,就是规则 90。

一般地,假设元胞自动机的规则半径为 r,对于只有两个状态的元胞,构造双触发元胞自动机的步骤如下:令 $0\leqslant i\leqslant 2^{2r-1}$,$b$ 表示任意二进制位串的位,在双触发模式下,b 每读一位,若 $b=0$,则相应规则表的第 $2i$ 项置为 0,第 $2i+1$ 项置为 1,第 $2i+2^{2r}$ 项置为 1,第 $2i+2^{2r}+1$ 项置为 0;若 $b=1$,相应规则表的第 $2i$ 项置为 1,第 $2i+1$ 项置为 0,第 $2i+2^{2r}$ 项置为 0,第 $2i+2^{2r}$ 项置为 1。因此,规则半径 $r=1$ 时,位串为"0,0",构造出了规则 90;位串为"0,1",构造出了规则 105;位串为"1,0",构造出了规则 150;位串为"1,1",构造出了规则 165。表 1 给出了半径为 1 时的双触发元胞自动机规则表。

表 1 半径 $r=1$ 时双触发元胞自动机的规则表

Index	90	105	150	165
000	0	1	0	1
001	1	0	1	0
010	0	0	1	1
011	1	1	0	0
100	1		1	0
101	0	1	0	1
110	1	1	0	0
111	0	0	1	1

3.3 耦合双触发元胞自动机的设计

与耦合单触发元胞自动机类似,耦合双触发元胞自动机密码系统采用耦合双触发元胞自动机规则作为密钥,将明文编码作为初始状态,反向演化一定时步得到的状态即构成密文;接收方收到密文后,正向迭代这个不可逆 CA 系统,经过与加密时相同的演化时步,恢复明文。

3.3.1 加密系统

明文经编码器编码成两列长度都为 N 的二进制位串,用随机源生成 $4r$ 位随机数。与单触发元胞自动机不同,注入的随机数并非固定添加在明文编码的一侧,而是可以随机选择一个位置,这也是双触发规则的性质决定的。在一列明文中插入 $2r$ 位随机数,同时分别存储在 $Ra1$、$Ra2$ 两个寄存器中,在另外一个明文中同样位置插入 $2r$ 位随机数,并存储在 $Rb1$、$Rb2$ 两个寄存器中。在插入随机数的两侧分别指定一个指针,即 $k1=ai$,$k2=ai+1$,其中 $k1$ 向左侧演化,$k2$ 向右侧演化。向左演化利用元胞自动机左触发的性质,向右演化利用元胞自动机右触发的性质。在计算指针 $k1$ 对应元胞的先导状态值时,根据该元胞当前状态值、寄存器 $Ra1$ 中 $r_{a0}\cdots r_{ar-1}$,$r_{ar}\cdots r_{a2r+1}$ 以及 $Rb1$ 中的 r_{br-1} 的值,从规则表中的相应规则得到元胞的先导状态值。同时移位寄存器 $Ra1$、$Rb1$ 右移一位,将 f,g 的值分别置入 $Ra1$、$Rb1$ 的左侧。然后指针 $k1$ 左移一位,重复上述步骤,直到 $k1=0$,完成一轮左触发加密操作。在计算指针 $k2$ 对应元胞的先导状态值时,与上面的方法类似,只是利用元胞自动机的右触发性质,向右运行。计算指针 $k2$ 对应元胞的先导状态值时,根据该元胞当前状态值、寄存器 $Ra2$ 中 $r'_{a0}\cdots r'_{ar-1}$,$r'_{ar}\cdots r'_{a2r+1}$ 以及 $Rb2$ 中 r'_{br-1} 的值,从规则表中的相应规则得到元胞的先导状态值。同时移位寄存器 $Ra2$、$Rb2$ 左移一位,将 f,g 的值分别置入 $Ra2$、$Rb2$ 的右侧。然后指针 $k2$ 右移一位,重复上述步骤,直到 $k2=N+2r-1$,完成一轮右触发加密操作。每轮中每个 CA 都会有 $2r$ 位随机数注入,因此完成 n 轮数据加密后的整个数据总数就是 $2N+2*2(n+1)r$。加密过程如图 1 所示。

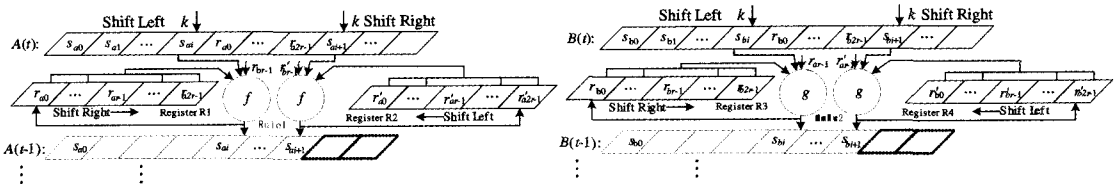


图 1　耦合双触发元胞自动机数据加密过程

3.3.2　解密系统

接收方收到密文后需要进行解密，解密的过程完全是个并行的过程，可以进行并行操作。步骤如下：运用同样的动力系统对密文的状态进行运算，首先生成一个解密指针 k。若用 q 表示最右端数据，则 $k=q-2r$。根据所 k 指的元胞以及元胞 $k-2r,\cdots,k-1$ 的值从规则表中确定 f 和 g 的值，把这个值赋给 k 的下一时刻的值，并把 k 值减 1，重复上述步骤直到 $k=1$，完成一轮迭代。执行与加密的同样的 n 轮解密，即可得到明文编码，合并后经解码器得到明文信息。解密过程如图 2 所示。

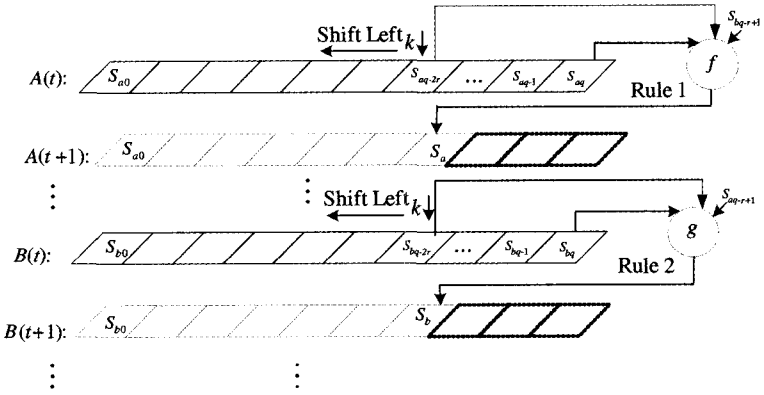


图 2　耦合双触发元胞自动机数据解密过程

4　仿真实验与安全性分析

4.1　仿真实验

以最简单的规则半径 $r=1$ 的双触发耦合元胞自动机为例，对明文“hello world”进行加密。首先进行编码，明文对应的 ASCII 码为“01101000 01100101 011011 0001101100 0110111100 100000 011101 1101101 111011 10010 0110110000111 00100”。将这些 ASCII 码分为等长的两部分，作为耦合元胞自动机的两个初始状态。对规则半径为 1 的双触发元胞自动机，共有 90、105、150 和 165 四种双触发规则。在仿真实验中，我们选择规则 165 和规则 150 作为密钥，加密轮数选为 8。运行耦合元胞自动机系统 8 轮完成加密，得到最后的密文二进制是“0001100001011001100011111100001100011100010100001000 1100100 0010101010111011010100100000 1101101000101100110001100110”。解密过程按 (R_1,R_2,n)，即(165,150,8)完成密文的解密，合并后经解码得到最终明文“hello world”。简单耦合元胞自动机系统的加密和解密过程如表 2～5 所示，其中的粗体表示每轮中加入的随机数。

表 2　耦合双触发元胞自动机中 A 的加密过程

Rule	Step	Cellular Automata A's encryption
165	0	01101000011001010111011000110110001111 0010
165	1	11010001100001110111101001111010011110101 00100
165	2	10100011010011010111111101101010001111111011100011
165	3	10111001011100001000000001011101100000000101001111
165	4	10111110001010011011001100100000101100110010001111111
165	5	00010101001110110100001111000110010000111100011010101 0
165	6	01100010001111101000110000001101001001101010011110111011
165	7	10000110110000000010011110011000010010010111011010100000101
165	8	00011000010110011000111111000011000111000101000010001100100 0

表 3　耦合双触发元胞自动机中 B 的加密过程

Rule	Step	Cellular Automata B's encryption
150	0	0000011101110110111011101100100110110001100100
150	1	0100011100101011001100111111010110000011110100
150	2	1100110010111100101001010010000001101010110010 00
150	3	0001010100100000101110001011010000101110110100000 0
150	4	0010111000101001010111111010100010001110010010000000
150	5	0011001001110101010111100110110110011011010110001000 10
150	6	0000001011001110011100101101011111110111100111010101 01
150	7	1100111111011010111110100100001011110110110110000000100000
150	8	0101010101111011010100100000110110100101001010110110001101 10

表 4　耦合双触发元胞自动机中 A 的解密过程

Rule	Step	Cellular Automata A's decryption
165	0	0001100001011001100011111100001100011100010100001000110010 00
165	1	1000011011000000001001111001100001001001011101101010000 0101
165	2	0110001000111110100011000000110100100110101001111011 1011
165	3	0001010100111011010000111100011001000011111000110101010
165	4	1011111000101001101100110010000010110011001000111111
165	5	1011100101110000100000000101110110000000001010011 11
165	6	1010001101001101011111101101010001111110111000 11
165	7	1101000110000111011110100111101001111010100100
165	8	0110100001100101011011000110110001110111 10010

表 5　耦合双触发元胞自动机中 B 的解密过程

Rule	Step	Cellular Automata B's decryption
150	0	0101010101111011010100100000110110100101001010110110001101 10
150	1	1100111111011010111110100100001011110110110110000000100000
150	2	0000001011001110011100101101011111110111100111010101 01
150	3	0011001001110101010111100110110110011011010110001000 10
150	4	0010111000101001010111111010100010001110010010000000
150	5	0001010100100000101110001011010000101110110100000 0
150	6	1100110010111100101001010010000001101010110010 00
150	7	0100011100101011001100111111010110000011110100
150	8	0000011101110110111011100100110110001100100

这里只是对最简单情况进行一下仿真演示。由于加解密的速度非常快，因此在实际应用中，规则半径通常要取 $r>10$ 以上，以达到实用的安全强度。

4.2 安全性分析

安全性分析中很重要的一项就是研究明文或密文改变一位后密文和明文的变化。通常采用改变一位明文编码后最终密文的改变结果与原来的加密结果进行比较，如果相同则用"-"表示，不同则用"#"表示。表 6～7 给出在相同明文中的相同扰乱引起的误差传播过程的比较。

表 6 耦合单触发元胞自动机中的误差传播

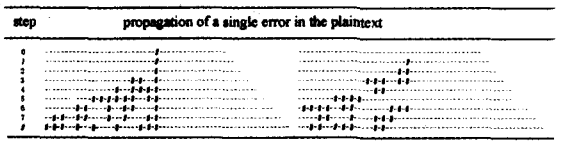
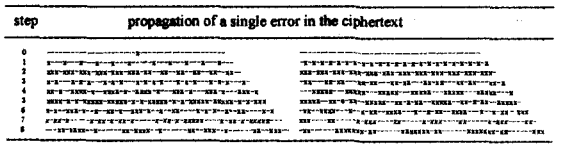


表 7 耦合双触发元胞自动误差传播



从表 6～7 可以看出，这种方法可以大大提高对密文的扰乱程度，只要几步就可以使误差扩展到整个密文，避免密文中的相似性问题，从而能够抵抗差分分析方法攻击。

在加密和解密过程中，密钥采用 CA 系统本身，当半径 $r=4$ 时，密钥空间达 $2^{2^{2r-1}}\times 2^{2^{2r-1}}\approx 1.16\times 10^{77}$。在相同的规则半径下，远远大于目前所见文献中提到的本类方法的密钥空间[10]。而且密钥空间随着规则半径 r 的增大呈指数增长。因为 CA 的并行特性，其加解密速度较快，在实际应用中，规则半径应选取 $r>10$，蛮力攻击变得不可能，系统在计算上是安全的。对同一明文加密，由于每次引入不同的随机数，因此每次得到的密文是不同的，但是解密后得到的明文却是相同的，很难得到唯一的明文密文对，因而可以抵抗已知明文和已知密文的攻击。

结论 本研究基于元胞自动机之间状态演化的互动性，以及触发元胞状态值与规则半径对演化状态的支配性，构造出耦合双触发元胞自动机的加密系统。解决了通常触发元胞自动机的加密算法中误差传播小而且是单向的相似性问题，同时大大提高密钥空间。分析表明，这样不仅具有抵抗穷举法的蛮力攻击和已知明文、已知密文的攻击的能力，同时具有抵抗差分分析的能力。

参 考 文 献

1 Lai C. High-speed cellular-automata based block cipher and fault tolerant public-key cryptosystems: [M. Sc.]. Regina: The University of Regina, Canada, 2000

2 Wolfram S. A New Kind of Science. Illinois: Wolfram Media, Inc, 2002. 1192

3 Martin del Rey A. A Novel Cryptosystem for Binary Images. Studies in Informatics and Control, 2004, 13(1): 5～14

4 Li H, Zhang C N. A Cellular Automata Based Reconfigurable Architecture for Hybrid Cryptosystems. Computer Journal, 2004, 47(3): 320～328

5 Seredynski F, Bouvry P, Zomaya A Y. Cellular automata computations and secret key cryptography. Parallel Computing, 2004, 30(5-6): 753～766

6 Oliveira G M B, Coelho A R, Monteiro L H A. Cellular automata cryptographic model based on bi-directional toggle rules. International Journal of Modern Physics C, 2004, 15(8): 1061～1068

7 Gutowitz H A. Method and apparatus for encryption, decryption and authentication using dynamical systems. USA, 1994. 34

8 Chopard B, Droz M. 物理系统的元胞自动机模拟. 祝玉学，赵学龙译. 北京：清华大学出版社，2003

9 赵学龙. 耦合触发元胞自动机在数据加密中的应用. 信息与控制，2005,34(6):746～752

10 张传武，沈野樵，彭启琮. 细胞自动机反向迭代加密技术研究. 计算机学报，2004，27(1)：125～129

（上接第 44 页）

4 SSF 模型测试

本模型的建立从理论上实现了灵活业务和基本呼叫的分离，并且以简约的模型使业务控制效率不会在 SSF 这一层受到制约。在试验中，以此模型建立 SSF，作为以高级业务功能为代表的 ACP 和以基本业务为代表的 BCP 的中间层，形成 ACP-SSF-BCP 的整体模型，成功地完成了各项补充业务，在呼叫效率上也达到了试验的目的。下面的图例说明了实现的补充业务中消耗在 SSF 这一层所需要花费的微秒值(图 4)。

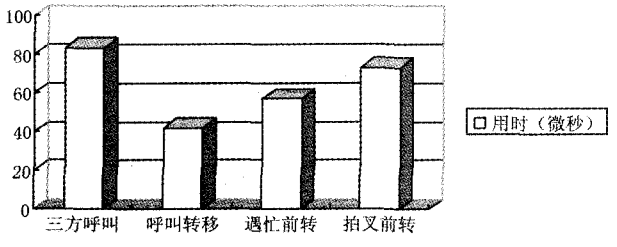


图 4 业务效率图

结论 软交换是下一代通信网络的核心控制设备，其中又以呼叫模块为其核心。在半呼叫为核心的网络中，上述的 SSF 模型很好地完成了 SCF 和 CCF 之间的桥梁作用。以单点控制为核心，以上下两条命令流程为建立模型基础，清晰简约地解决了 SSF 所面临的多种问题，并以 TDP 表的方式解决了单业务的触发问题，以 EDP 表的方式解决了业务的控制问题，以 CDP 表的方式解决了多业务的冲突问题，最后以 SESSION 为子模块的设计解决了多业务的并发问题。经过实践的证明，这样的 SSF 模型是一种合理的、可靠的设计。

参 考 文 献

1 Lu Huilan. Network evolution in the context of the global information infrastructure. Communications Magazine, 1998, 36(8): 98～102

2 Huitema C. An architecture for residential Internet telephony service. IEEE Network, 1999, 13(5): 50～56

3 Rosenberg J. Session initiation protocol. RFC3261, Intrnet Engineering Task Force, June 2002

4 Cuervo F. *Megaco Protocol Version 1. 0. RFC3015*, November 2000

5 Ong L, Rytina I, Garcia M. Framework Architecture for Signaling Transport. RFC2719, Internet Engineering Task Force, October 1999

6 中华人民共和国邮电部.《中国智能网设备业务交换点(SSP)技术规范》