完善保密方案中的优先退化协议

胡予濮[1], 杨 波[1], 张玉清[2]
(1. 西安电子科技大学 ISN 国家重点实验室, 信息安全研究所, 陕西西安 710071; 2. 清华大学信息网络工程研究中心, 北京 100084)

摘 要: 本文给出一类新的完善保密协议——优先退化协议, 它与以往的优先提取协议具有不同的功能: 优先提取是指通信伙伴的互信息被首先提取, 而优先退化是指敌方掌握的信息被首先退化. 本文讨论了优先退化协议有效的条件, 并给出了一个同时具有优先提取和优先退化功能的混合协议.

关键词: 完善保密; 密钥协商; 优先提取; 保密增强
中图分类号: TN918.4 文献标识码: A 文章编号: 0372-2112 (2002) 04-0533-03

An Advantage Degeneration Protocol in Complete Security Scheme

HU Yu-pu[1], YANG Bo[1], ZHANG Yu-qing[2]
(1. *ISPI, ISN National Key Lab., Xidian University, Xi'an, Shaanxi 710071, China*; 2. *Qinghua Vniversity, Beijing 100084, China*)

Abstract: This paper presents a new class of complete security protocol——advantage degeneration protocol. Advantage degeneration protocol and former advantage distillation protocol have different functions: one means that the mutual information of communication partners is distilled firstly, another that the information of enemy is degenerated firstly. The paper discusses conditions for efficient protocol, and presents a mixed protocol which has both advantage distillation and advantage degeneration functions.

Key words: complete security; key agreement; advantage distillation; privacy amplification

1 引言

信息保密有两个不同的概念: 完善保密和计算保密. 完善保密为一次一密制, 此时秘密信息对敌方来说是一个真正的随机变量; 计算保密为一次多密制, 此时秘密信息对敌方来说虽不是一个随机变量, 但敌方找不到有效的破译方法, 只能随机猜测(这相当于面对一个有解但难解的方程). 长期以来由于完善保密难以实现, 故人们在信息保密方面的努力主要集中在计算保密上. 近年来形势渐渐有所改变, 显示出了以下两个特征: (1) 人类计算能力越来越强, 其中包括芯片技术的飞速发展和量子计算机的问世, 这一切预示着"计算保密"似乎越来越不可靠. (2) 大量有扰信道(比如卫星信道和广播信道)的开通, 使得通信伙伴之间能够共享源源不断的互信息; 只要使用信息处理技术, 将这些互信息中敌手已知的部分去掉, 保留并协调敌手未知的部分, 通信伙伴之间就获得了源源不断的密钥流, 因而实现了一次一密, 达到"完善保密".

从通信伙伴的互信息中获取完善保密的密钥流, 又称为密钥协商. 它可分为优先提取、信息协调、保密增强三个步骤[1]. 优先提取是指通信伙伴的互信息被首先提取, 而敌方所掌握的信息不被提取或晚一步被提取; 信息协调是指通信伙伴的互信息被首先提取, 而敌方所掌握的信息不被提取或晚一步被提取; 信息协调是指通信伙伴的互信息被进一步纠错; 保密增强是指将敌方所掌握的信息进行退化. M J Gander 和 U M Maurer[2,3] 提出了一个比特对检验协议, 这是迄今为止最有效的优先提取协议. 协议描述如下.

设 Alice 拥有一个对称分布无记忆比特串 $X = X_1X_2\cdots$(即随机变量 X_1、X_2、…相互独立, 各自等概地取值 0 和 1). 比特串 X 分别通过两个相互独立的 BSC 信道(二元对称无记忆信道)发送给 Bob 和 Eve, Bob 收到比特串 $Y = Y_1Y_2\cdots$, Eve 收到比特串 $Z = Z_1Z_2\cdots$, 向 Bob 和 Eve 发送的误比特率分别为 p 和 q(即有条件概率 $P(Y_k \neq x \mid X_k = x) = p$, $P(Z_k \neq x \mid X_k = x) = q$), $0 < p < 1/2$, $0 < q < 1/2$. Alice 和 Bob 通过一条无扰的可认证信道交换信息(Eve 在这条信道上只能截听). 对于 $k = 1, 2, \cdots$, Alice 计算 $U_k = X_{2k-1} + X_{2k}$, 并将 U_k 发送给 Bob; Bob 计算 $V_k = Y_{2k-1} + Y_{2k}$, 并将 V_k 发送给 Alice. 如果 $V_k = U_k$, 则 Alice 删去自己比特中中的 X_{2k}, Bob 删去自己比特串中的 Y_{2k}; 如果 $V_k \neq U_k$, 则 Alice 删去自己比特串中的 $X_{2k-1}X_{2k}$, Bob 删去自己比特串中的 $Y_{2k-1}Y_{2k}$. 这样 Alice 获得了删减后的比特串 $X^{(1)} = X^{(1)}X^{(1)}2\cdots$; Bob 获得了删减后的比特串 $Y^{(1)} = Y_1^{(1)}Y_2^{(1)}\cdots$; Eve 也通过截听对应地获得了删减后的比特串 $Z^{(1)} = Z_1^{(1)}Z_2^{(1)}\cdots$.

引理[2,3] 设比特串 $X^{(1)}$ 与 $Y^{(1)}$ 的误比特率为 $p^{(1)}$, 比特串 $X^{(1)}$ 与 $Z^{(1)}$ 的误比特率为 $q^{(1)}$. 则 $p^{(1)} = p^2/[(1-p)^2 + p^2] < p$; $q^{(1)} = q$.

将以上的交互计算过程重复 n 次后, Alice 获得了删减比特串 $X^{(n)} = X_1^{(n)}, X_2^{(n)}, \cdots$; Bob 获得了删减比特串 $Y^{(n)} = Y_1^{(n)}, Y_2^{(n)}\cdots$; Eve 通过截听获得了删减比特串 $Z^{(n)} = Z_1^{(n)}, {}_2^{(n)}, \cdots$. 设比特串 $X^{(n)}$ 与 $Y^{(n)}$ 的误比特率为 $p^{(n)}$, 比特串 $X^{(n)}$ 与 $Z^{(n)}$ 的误比特率为 $q^{(n)}$, 则容易证明 $p^{(n)} = \dfrac{(p/(1-p))^{2^n}}{1 + (p/(1-p))^{2^n}}$; $q^{(n)} = q$.

本文给出一类新的完善保密协议——优先退化协议, 它与 M J Gander 和 U M Maurer 的优先提取协议具有不同的功能: 优先提取是指通信伙伴的互信息被首先提取, 而优先退化

收稿日期: 2000-10-10; 修回日期: 2001-04-06
基金项目: 国家自然科学基金(No. 69972034); 高等学校国家重点实验室访问学者基金

是指敌方掌握的信息被首先退化. 我们构造的优先退化协议如同 M J Gander 和 U M Maurer 的优先提取协议一样简易, 没有任何实质性的计算, 且该协议有效所需的条件是很弱的.

本文还给出一个同时具有优先提取和优先退化功能的混合协议, 而优先退化的实际含义就是保密增强. 只要初始的 $p \leqslant 0.292893$ 就能使协议运行, 且在迭代过程中每一轮 p 至少是折半递减趋于 0, q 单调趋于 1/2. 当 p 在 0.11~0.29 范围内时, p 递减而 q 不变, 即此时只有提取功能而没有退化功能. 当 $p \leqslant 0.1$ 时, 就同时具有提取和退化功能; p 越小, 退化功能越强.

2 优先退化协议

在以下的叙述中, 记号 $P(\cdot)$ 总表示概率, $P(\cdot|\cdot)$ 总表示条件概率. 仍设 Alice 拥有一个对称分布无记忆比特串 $X = X_1, X_2, \cdots$. 比特串 X 分别通过两个相互独立的 BSC 信道发送给 Bob 和 Eve, Bob 收到比特串 $Y = Y_1, Y_2, \cdots$, Eve 收到比特串 $Z = Z_1, Z_2, \cdots$, 向 Bob 和 Eve 发送的误比特率分别为 p 和 q, $0 < p < 1/2$, $0 < q < 1/2$. 仍设 Alice 和 Bob 通过一条无扰的可认证信道交换信息.

对于 $k = 1, 2, \cdots$, Alice 计算 $U_k = \sum_{j=0}^{2m-1} X_{2mk-j}$, 并将 U_k 发送给 Bob; Bob 计算 $V_k = \sum_{j=0}^{2m-1} Y_{2mk-j}$, 并将 V_k 发送给 Alice. 如果 $V_k = U_k$, 则 Alice 计算并保留一个比特 $\sum_{j=m}^{2m-1} X_{2mk-j}$, 同时删去自己原先比特串中的 $X_{2m(k-1)+1}, X_{2m(k-1)+2}, \cdots, X_{2mk}$; Bob 计算并保留一个比特 $\sum_{j=m}^{2m-1} Y_{2mk-j}$, 同时删去自己原先比特串中的 $Y_{2m(k-1)+1}, Y_{2m(k-1)+2}, \cdots, Y_{2mk}$. 如果 $V_k \neq U_k$, 则 Alice 删去自己原先比特串中的 $X_{2m(k-1)+1}, X_{2m(k-1)+2}, \cdots, X_{2mk}$; Bob 删去自己原先比特串中的 $Y_{2m(k-1)+1}, Y_{2m(k-1)+2}, \cdots, Y_{2mk}$. 这样 Alice 获得了合并/删减后的比特串 $X^{(1)} = X_1^{(1)} X_2^{(1)} \cdots$; Bob 获得了合并/删减后的比特串 $Y^{(1)} = Y_1^{(1)} Y_2^{(1)} \cdots$; Eve 也通过截听获得了合并/删减后的比特串 $Z^{(1)} = Z_1^{(1)} Z_2^{(1)} \cdots$.

定理 1 设比特串 $X^{(1)}$ 与 $Y^{(1)}$ 的误比特率为 $p^{(1)}$, 比特串 $X^{(1)}$ 与 $Z^{(1)}$ 的误比特率为 $q^{(1)}$. 则 $p^{(1)} = \left(\frac{1-(1-2p)^m}{1+(1-2p)^m}\right)^2 \Big\backslash \left\{1+\left(\frac{1-(1-2p)^m}{1+(1-2p)^m}\right)^2\right\}$; $q^{(1)} = \frac{1-(1-2q)^m}{2} > q$.

证明 取 Alice 的比特串 $A = A_1, A_2, \cdots$, Bob 的比特串 $B = B_1 B_2 \cdots$, Eve 的比特串 $C = C_1 C_2 \cdots$, 其中 $A_k = \sum_{j=1}^{m} X_{m(k-1)+j}$, $B_k = \sum_{j=1}^{m} Y_{m(k-1)+j}$, $C_k = \sum_{j=1}^{m} Z_{m(k-1)+j}$. 比特串 A 与 B 的误比特率 r 为条件概率:

$$r = P\left(\sum_{j=1}^{m} Y_j \neq x \,\middle|\, \sum_{j=1}^{m} X_j = x\right)$$

$= P(X_1, X_2, \cdots, X_m$ 与 $Y_1, Y_2, \cdots, Y_m$ 之间比特的个数为奇数$\left| \sum_{j=1}^{m} X_j = x\right)$

$= P(X_1, X_2, \cdots, X_m$ 与 $Y_1, Y_2, \cdots, Y_m$ 之间误比特的个数为奇数$)$

$$= \frac{1}{2}\sum_{j=0}^{\lfloor m/2 \rfloor} C_m^{2j} p^{2j} (1-p)^{m-2j} = \frac{1-(1-2p)^m}{2};$$

同理, 比特串 A 与 C 的误比特率 s 为条件概率: $s = P\left(\sum_{j=1}^{m} Z_j \neq x \,\middle|\, \sum_{j=1}^{m} X_j = x\right) = \frac{1-(1-2q)^m}{2}$. 另外, 有 $P(A_{2i-1} + A_{2i} \neq B_{2i-1} + B_{2i}) = 2r(1-r)$.

以下计算 $X^{(1)}$ 与 $Y^{(1)}$ 的误比特率 $p^{(1)}$, 以及 $X^{(1)}$ 与 $Z^{(1)}$ 的误比特率 $q^{(1)}$.

$$\begin{aligned}
p^{(1)} &= P(Y_1^{(1)} \neq x \,|\, X_1^{(1)} = x) \\
&= \sum_{k=1}^{+\infty} P(Y_1^{(1)} \neq x; A_{2i-1} + A_{2i} \neq B_{2i-1} + B_{2i}, i = 1 \sim k-1; \\
&\qquad A_{2k-1} + A_{2k} = B_{2k-1} + B_{2k} \,|\, X_1^{(1)} = x) \\
&= 2\sum_{k=1}^{+\infty} P(A_{2i-1} + A_{2i} \neq B_{2i-1} + B_{2i}, i = 1 \sim k-1; \\
&\qquad A_{2k-1} = x \neq B_{2k-1}; A_{2k} \neq B_{2k}) \\
&= \sum_{k=1}^{+\infty} P(A_{2i-1} + A_{2i} \neq B_{2i-1} + B_{2i}, i = 1 \sim k-1; \\
&\qquad A_{2k-1} \neq B_{2k-1}; A_{2k} \neq B_{2k}) \\
&= \sum_{k=1}^{+\infty} P(A_{2k-1} \neq B_{2k-1}) P(A_{2k} \neq B_{2k}) \prod_{i=1}^{k-1} P(A_{2i-1} + A_{2i} \\
&\qquad \neq B_{2i-1} + B_{2i}) = r^2 \sum_{k=1}^{+\infty} (2r(1-r))^{k-1} = \frac{r^2}{(1-r)^2 + r^2}
\end{aligned}$$

注意到比特串 B 与 C 关于比特串 A 条件独立(这是因为比特串 X 分别通过两个相互独立的 BSC 信道发送, 分别收到比特串 Y 和比特串 Z), 因此有 $q^{(1)} = s$. 定理 1 得证.

推论 1 将以上的交互计算过程重复 n 次后, Alice 获得了合并/删减后的比特串 $X^{(n)} = X_1^{(n)}, X_2^{(n)}, \cdots$; Bob 获得了合并/删减后的比特串 $Y^{(n)} = Y_1^{(n)}, Y_2^{(n)}, \cdots$; Eve 通过截听获得了合并/删减后的比特串 $Z^{(n)} = Z_1^{(n)}, Z_2^{(n)}, \cdots$. 设比特串 $X^{(n)}$ 与 $Y^{(n)}$ 的误比特率为 $p^{(n)}$, 比特串 $X^{(n)}$ 与 $Z^{(n)}$ 的误比特率为 $q^{(n)}$, 则

$$p^{(n)} = \left(\frac{1-(1-2p)^m}{1+(1-2p)^m}\right)^{2^n} \Big\backslash \left\{1+\left(\frac{1-(1-2p)^m}{1+(1-2p)^m}\right)^{2^n}\right\};$$

$$q^{(n)} = \frac{1-(1-2q)^{m^n}}{2}.$$

从定理 1 和推论 1 知, 随着优先退化协议重复执行次数 n 的增大, $q^{(n)}$ 迅速地单调收敛于 1/2, 即比特串 $Z^{(n)}$ 与比特串 $X^{(n)}$ 趋于不相关; $p^{(n)}$ 迅速地收敛于 0, 即比特串 $Y^{(n)}$ 与比特串 $X^{(n)}$ 趋于一致. 现在的问题是, $p^{(n)}$ 是否也单调收敛? 这就是说, 是否每执行一次优先退化协议都能够使 Eve 和 Alice 各自比特串的相关性明显退化, 而 Bob 和 Alice 各自比特串的相关性至少不退化? 首先指出以下一个事实:

命题 设 $p^{(n)}$ 为推论 1 所述, $n = 0, 1, 2, \cdots$. (1) 若有某个 N 使 $p^{(N)} \geqslant p^{(N+1)}$, 则序列 $\{p^{(N)}, p^{(N+1)}, p^{(N+2)}, \cdots\}$ 是单调减序列; (2) 若有某个 M 使当 $m = M$ 时有 $p^{(0)} = p \geqslant p^{(1)}$, 则当 $m = 1, 2, \cdots, M-1$ 时总有 $p^{(0)} \geqslant p^{(1)}$.

根据这一命题, 只需要寻找最大的正整数 m 使得 $p \geqslant$

$p^{(1)}$, 就可以在限制 $p^{(n)}$ 单调减的前提下, 保证 $q^{(n)}$ 最快地收敛于 1/2. 下面的表 1 列出了 p 取各值时, 满足 $p \geqslant p^{(1)}$ 的最大正整数 m 的对应值.

表 1　p 的值以及满足 $p \geqslant p^{(1)}$ 的最大正整数 m 的对应值

p 的范围	最大 m	p 的范围	最大 m
$0 < p \leqslant 0.00010000$	≥100	0.00038443~ 0.00039995	50
0.00010001~ 0.00010203	99	0.00039996~ 0.00041644	49
0.00010204~ 0.00010412	98	0.00041645~ 0.00043396	48
0.00010413~ 0.00010628	97	0.00043397~ 0.00045263	47
0.00010629~ 0.00010850	96	0.00045264~ 0.00047252	46
0.00010851~ 0.00011080	95	0.00047253~ 0.00049375	45
0.00011081~ 0.00011317	94	0.00049376~ 0.00051644	44
0.00011318~ 0.00011562	93	0.00051645~ 0.00054074	43
0.00011563~ 0.00011814	92	0.00054075~ 0.00056679	42
0.00011815~ 0.00012075	91	0.00056680~ 0.00059477	41
0.00012076~ 0.00012345	90	0.00059478~ 0.00062487	40
0.00012346~ 0.00012624	89	0.00062488~ 0.00065732	39
0.00012625~ 0.00012913	88	0.00065733~ 0.00069236	38
0.00012914~ 0.00013211	87	0.00069237~ 0.00073028	37
0.00013212~ 0.00013520	86	0.00073029~ 0.00077141	36
0.00013521~ 0.00013840	85	0.00077142~ 0.00081610	35
0.00013841~ 0.00014172	84	0.00081611~ 0.00086480	34
0.00014173~ 0.00014515	83	0.00086481~ 0.00091799	33
0.00014516~ 0.00014871	82	0.00091800~ 0.00097624	32
0.00014872~ 0.00015241	81	0.00097625~ 0.00104022	31
0.00015242~ 0.00015624	80	0.00104023~ 0.00111070	30
0.00015625~ 0.00016022	79	0.00111071~ 0.00118859	29
0.00016023~ 0.00016436	78	0.00118860~ 0.00127497	28
0.00016437~ 0.00016865	77	0.00127498~ 0.00137111	27
0.00016866~ 0.00017312	76	0.00137112~ 0.00147856	26
0.00017313~ 0.00017777	75	0.00147857~ 0.00159915	25
0.00017778~ 0.00018260	74	0.00159916~ 0.00173511	24
0.00018261~ 0.00018764	73	0.00173512~ 0.00188917	23
0.00018765~ 0.00019289	72	0.00188918~ 0.00206469	22
0.00019290~ 0.00019836	71	0.00206470~ 0.00226586	21
0.00019837~ 0.00020407	70	0.00226587~ 0.00249792	20
0.00020408~ 0.00021003	69	0.00249793~ 0.00276752	19
0.00021004~ 0.00021625	68	0.00276753~ 0.00308324	18
0.00021626~ 0.00022275	67	0.00308325~ 0.00345621	17
0.00022276~ 0.00022955	66	0.00345622~ 0.00390116	16
0.00022956~ 0.00023667	65	0.00390117~ 0.00443786	15
0.00023668~ 0.00024412	64	0.00443787~ 0.00509336	14
0.00024413~ 0.00025193	63	0.00509337~ 0.00590548	13
0.00025194~ 0.00026012	62	0.00590549~ 0.00692835	12
0.00026013~ 0.00026872	61	0.00692836~ 0.00824167	11
0.00016873~ 0.00027775	60	0.00824168~ 0.00996662	10
0.00027776~ 0.00028725	59	0.00996663~ 0.01229479	9
0.00028726~ 0.00029724	58	0.01229480~ 0.01554345	8
0.00029725~ 0.00030776	57	0.01554346~ 0.02026894	7
0.00030777~ 0.00031884	56	0.02026895~ 0.02751959	6
0.00031885~ 0.00033054	55	0.02751960~ 0.03946366	5
0.00033055~ 0.00034290	54	0.03946366~ 0.06118605	4
0.00034291~ 0.00035596	53	0.06118606~ 0.10692431	3
0.00035597~ 0.00036978	52	0.10692432~ 0.22815549	2
0.00036979~ 0.00038442	51	0.22815550~ 0.49999999	1

3　优先提取/优先退化的混合协议

保留上述关于 Alice、Bob 和 Eve 的一切假设. 协议如下.

步骤 **1**　Alice 寻找最大的正整数 m, 使得 $p^{(1)} = \left(\frac{1-(1-2p)^m}{1+(1-2p)^m}\right)^2 \Big\backslash \left\{1+\left(\frac{1-(1-2p)^m}{1+(1-2p)^m}\right)^2\right\} \leq \frac{p}{2}$, 并将 m 发送给 Bob.

步骤 **2**　对于 $k = 1, 2, \cdots$, Alice 计算 $U_k = \sum_{j=0}^{2m-1} X_{2mk-j}$, 并将 U_k 发送给 Bob; Bob 计算 $V_k = \sum_{j=0}^{2m-1} Y_{2mk-j}$, 并将 V_k 发送给 Alice.

步骤 **3**　如果 $V_k = U_k$, 则 Alice 计算并保留一个比特 $\sum_{j=m}^{2m-1} X_{2mk-j}$, 同时删去自己原先比特串中的 $X_{2m(k-1)+1}, X_{2m(k-1)+2}, \cdots, X_{2mk}$. Bob 计算并保留一个比特 $\sum_{j=m}^{2m-1} Y_{2mk-j}$, 同时删去自己原先比特串中的 $Y_{2m(k-1)+1}, Y_{2m(k-1)+2}, \cdots, Y_{2mk}$. 如果 $V_k \neq U_k$, 则 Alice 删去自己原先比特串中的 $X_{2m(k-1)+1}, X_{2m(k-1)+2}, \cdots, X_{2mk}$; Bob 删去自己原先比特串中的 $Y_{2m(k-1)+1}, Y_{2m(k-1)+2}, \cdots, Y_{2mk}$. 这样 Alice 获得了合并/删减后的比特串 $X^{(1)}$; Bob 获得了合并/删减后的比特串 $Y^{(1)}$ (Eve 也通过截听获得了合并/删减后的比特串 $Z^{(1)}$).

步骤 **4**　令 $p = p^{(1)}, X^{(1)} = x, Y^{(1)} = y, q = \frac{1-(1-2q)^m}{2}$. 如果 $p \leqslant \delta$ 与 $1/2 - q \leqslant \delta$ 有一个不成立, 则转步骤 1; 否则停止.

如果这一协议能够运行, 则运行每一轮(即从步骤 1 运行到步骤 4)后 Alice 和 Bob 各自的串的误比特率降低了至少一半, 同时使 Alice 和 Eve 各自的串的误比特率提高. 问题是 p 为何值时协议能够运行一轮. 这里需要指出, 如果协议能够运行第一轮, 则必能够运行完毕. 能够运行第一轮的条件是对初始的 p 存在正整数 m, 使得 $\left(\frac{1-(1-2p)^m}{1+(1-2p)^m}\right)^2 \Big\backslash \left\{1+\left(\frac{1-(1-2p)^m}{1+(1-2p)^m}\right)^2\right\} \leq \frac{p}{2}$, 即初始的 p 要满足不等式 $p^2[(1-p)^2 + p^2] \leq p/2$. 由此得 $p \leqslant 0.292893$. 表 2 列出了 p 取各值时, 满足 $\left(\frac{1-(1-2p)^m}{1+(1-2p)^m}\right)^2 \Big\backslash \left\{1+\left(\frac{1-(1-2p)^m}{1+(1-2p)^m}\right)^2\right\} \leq \frac{p}{2}$ 的最大正整数 m 的对应值, 供步骤 1 使用.

表 2

p 的范围	0.001	0.002	0.003	0.004	0.005
最大的 m	20	15	12	11	9
p 的范围	0.006	0.007	0.008	0.009	0.010
最大的 m	9	8	7	7	7
p 的范围	0.015	0.02~ 0.03	0.05	0.06~ 0.10	0.11~ 0.29
最大的 m	5	4	3	2	1

4　结论

我们已经给出了一类新的完善保密协议——优先退化协议, 它与 M J Gander 和 U M Maurer 的优先提取协议具有不同的功能: 优先提取是指通信伙伴的互信息被首先提取, 而优先退化是指敌方掌握的信息被首先退化. 优先退化协议如同优先提取协议一样简易, 没有任何实质性的计算. 优先退化协议有效所需的条件是很弱的.

文[4]和[5]详细论述了密钥协商的理论和技术, 在那里密钥协商分为优先提取、信息协调、保密增强三个步骤. 本文第 3 节中给出了一个同时具有优先提取和优先退化功能的混合协议, 而优先退化的实际含义就是保密增强. 在这一节中我们看到, 只要初始的 $p \leqslant 0.292893$ 就能使协议运行, 且在迭代过程中每一轮 p 至少是折半递减趋于 0, q 单调趋于 1/2. 当 p 在 0.11~ 0.29 范围内时, p 递减而 q 不变, 即此时只有提取功能而没有退化功能. 当 $p \leqslant 0.1$ 时, 就同时具有提取和退化功能: p 趋小, 退化功能越强.

(下转第 543 页)

下着重讨论如何检测秘密分发者与秘密分享者的欺诈行为的. 若考虑秘密分发者与秘密分享者之间所传信息的认证功能, 以避免中间截获攻击, 可以采取签名或签密的办法[9] 对方案进行加强.

感谢　Ericsson 研究院 Rolf. J. Blum, Andras Mahes, Gorlan Selander 博士对本文初稿的建设性评论.

参考文献:

[1] E F Brickell, D M Daveport. On the classification of idea secret sharing scheme [J]. J Cryptology, 1991, 4(2): 123- 134.

[2] P A Fouque, G Poupard, J Stern. Sharing decryption in the context of voting or lotteries [A]. Proceedings of Financial Cryptography 2000 [C]. Berlin: Springer Verlag, 2000. 90- 104.

[3] M Tompa, H Woll. How to share a secret with cheaters [J]. Journal of Cryptology, 1988, 1(2): 133- 138.

[4] B Chor, S Goldwasser, S Micali, B Awerbuch. Veriable secret sharing and achieving simultaneity in the presence of faults[A]. Proceedings of 26th FOCS[C]. 1985. 251- 260.

[5] M Stadler. Publicly verifiable secret sharing [A]. Advances in cryptology- Eurocrypt' 96 [C]. Berlin: Springer Verlag, 1996. 190- 199.

[6] R G E Pinch. Online multiple secret sharing [J]. Electronics Letters, 1996, 32(12): 1087- 1088.

[7] R Gennaro, S Micali. Verifiable secret sharing as secure computation [A]. Advances in cryptology- Crypto' 94 [C]. Berlin: Springer Verlag, 1995. 168- 182.

[8] L Harn. Efficient sharing of multiple secrets [J]. IEE Proc Comput Digit Tech, 1995, 142(3): 237- 240.

[9] 张福泰, 王育民, 郑东. 用签密构造可验证秘密分享方案 [A]. CCICS' 2001 论文集 [C]. 北京: 科学出版社, 2001. 244- 248.

[10] F Boudot, J Traor'. Efficient publicly verifiable secret sharing schemes with fast or delayed recovery [A]. Lecture Notes in Computer Science 1726 [C]. Berlin: Springer Verlag, 1999. 87- 102.

作者简介:

何明星　男, 1964 年生于四川省南江县, 1990 年获重庆大学应用数学专业硕士学位, 现为四川工业学院计算机科学与工程系副教授, 西南交通大学计算机与通信工程学院通信与信息系统专业博士生, 主要研究兴趣为网络与信息安全、电子商务.

范平志　男, 1994 年获英国 Hull 大学通信工程专业博士学位, 现为西南交通大学计算机与通信工程学院教授, 博士生导师, IEEE 高级会员, 国家杰出青年基金获得者, 主要研究兴趣为移动通信、无线 IP、网络与信息安全.

(上接第 535 页)

参考文献:

[1] U M Maurer. Secret key agreement by public discussion from common information [J]. IEEE Trans IT, 1993, 39(3): 733- 742.

[2] M J Gander, U M Maurer. On the secret key rate of binary random variables [A]. Proc. of the 1994 IEEE Symp on Information Theory [C]. 1994. 351.

[3] U M Maurer. Protocols for secret key agreement based on common information [A]. Advances in Cryptology- CRYPTO' 92, Lecture Notes in Computer Science [C]. Berlin: Springer- Verlag, 1993. 740: 461- 470.

[4] Christian Cachin. Enropy measures and unconditional security in cryptography [D]. ETH, 1997.

[5] Stefan Wolf. Informationr theoretically and computationally secure key agreement in sryptography [D]. ETH, 1999.