文章编号：2096-1618(2016)02-0123-03
稿件来源：科学网
网　　址：http://blog.sciencenet.cn/blog-453322-948089.html
发表时间：2016-01-04

安全通论(3)

——攻防篇之“非盲对抗”之“石头剪刀布”

杨义先，　钮心忻
(北京邮电大学信息安全中心，北京 100876)

摘要：本文给出了“石头剪刀布”的一种“白富美”新玩法。所谓“白”，即思路清清楚楚、明明白白；所谓“富”，即理论内涵非常丰富；所谓“美”，即结论绝对数学美。《安全通论》的魅力也在这里得到了幽默体现。

0　引言

全人类，数千年来，都在玩“石头剪刀布”，而且，玩出了无尽幸福！

由浙江大学、浙江工商大学、中国科学院等单位组成的跨学科团队，在三百多名志愿者的配合下，历时4年，终于把“石头剪刀布”玩成了“高大上”：其成果被评为“麻省理工学院科技评论2014年度最优”，这也是中国社科成果首次入选该顶级国际科技评论。

本文利用《安全通论》，只需一张纸、一支笔，就把“石头剪刀布”玩成“白富美”。所谓“白”，即思路清清楚楚、明明白白；所谓“富”，即理论内涵非常丰富；所谓“美”，即结论绝对数学美。

不信？请读下文！

1　信道建模

设甲与乙玩“石头剪刀布”。他们可分别用随机变量 X 和 Y 来表示：

当甲出拳为剪刀、石头、布时，分别记为 $X=0$、$X=1$、$X=2$；

当乙出拳为剪刀、石头、布时，分别记为 $Y=0$、$Y=1$、$Y=2$。

根据概率论中的“大数定律”，频率的极限趋于概率，所以甲乙双方的出拳习惯，可以用随机变量 X 和 Y 的概率分布表示为：

$Pr(X=0)=p$，即，甲出“剪刀”的概率；

$Pr(X=1)=q$，即，甲出“石头”的概率；

$Pr(X=2)=1-p-q$，即，甲出“布”的概率。这里 $0<p,q,p+q<1$。

$Pr(Y=0)=r$，即，乙出“剪刀”的概率；

$Pr(Y=1)=s$，即，乙出“石头”的概率；

$Pr(Y=2)=1-r-s$，即，乙出“布”的概率。这里 $0<r,s,r+s<1$。

同样，还可以统计出二维随机变量 (X,Y) 的联合分布概率如下：

$Pr(X=0,Y=0)=a$，即，甲出“剪刀”，乙出“剪刀”的概率；

$Pr(X=0,Y=1)=b$，即，甲出“剪刀”，乙出“石头”的概率；

$Pr(X=0,Y=2)=1-a-b$，即，甲出“剪刀”，乙出“布”的概率。这里 $0<a,b,a+b<1$。

$Pr(X=1,Y=0)=e$，即，甲出“石头”，乙出“剪刀”的概率；

$Pr(X=1,Y=1)=f$，即，甲出“石头”，乙出“石头”的概率；

$Pr(X=1,Y=2)=1-e-f$，即，甲出“石头”，乙出“布”的概率。这里 $0<e,f,e+f<1$。

$Pr(X=2,Y=0)=g$，即，甲出“布”，乙出“剪刀”的概率；

$Pr(X=2,Y=1)=h$，即，甲出“布”，乙出“石头”的概率；

$Pr(X=2,Y=2)=1-g-h$，即，甲出“布”，乙出“布”的概率。这里 $0<g,h,g+h<1$。

由随机变量 X 和 Y，构造另一个随机变量 $Z=[2(1+X+Y)]\bmod 3$。由于任意两个随机变量都可构成一个通信信道，所以，以 X 为输入，以 Z 为输出，我们就得到一个通信信道 $(X;Z)$，称之为“甲方信道”。

如果在某次游戏中甲方赢，那么，就只可能有三种情况：

情况1，“甲出剪刀，乙出布”，即，“$X=0,Y=2$”，这也等价于“$X=0,Z=0$”，即，“甲方信道”的输入等于输

出;

情况 2,“甲出石头,乙出剪刀”,即,“$X=1,Y=0$”,这也等价于“$X=1,Z=1$”,即,“甲方信道”的输入等于输出;

情况 3,“甲出布,乙出石头”,即,“$X=2,Y=1$”,这也等价于“$X=2,Z=2$”,即,“甲方信道”的输入等于输出。

反过来,如果“甲方信道”将 1 比特信息成功地从发端送到了收端,那么,也只有三种可能的情况:

情况 1,输入和输出都等于 0,即,“$X=0,Z=0$”,这也等价于“$X=0,Y=2$”,即,“甲出剪刀,乙出布”,即,甲赢;

情况 2,输入和输出都等于 1,即,“$X=1,Z=1$”,这也等价于“$X=1,Y=0$”,即,“甲出石头,乙出剪刀”,即,甲赢;

情况 3,输入和输出都等于 2,即,“$X=2,Z=2$”,这也等价于“$X=2,Y=1$”,即,“甲出布,乙出石头”,即,甲赢。

综合以上正反两方面,共六种情况,就得到一个重要引理:

引理 1 甲赢一次,就意味着“甲方信道”成功地把 1 比特信息,从发端送到了收端;反之亦然。

再利用随机变量 Y 和 Z 构造一个信道 $(Y;Z)$,称之为“乙方信道”,它以 Y 为输入,以 Z 为输出。那么,仿照前面的论述,我们可得如下引理:

引理 2 乙方赢一次,就意味着“乙方信道”成功地把 1 比特信息,从发端送到了收端;反之亦然。

由此可见,甲乙双方玩“石头剪刀布”的输赢问题,就转化成了“甲方信道”和“乙方信道”能否成功地传输信息比特的问题。根据仙农第二定理[3],我们知道:信道容量就等于该信道能够成功传输的信息比特数。所以,“石头剪刀布”的游戏问题,就转化成了信道容量问题。更准确地说,我们有如下定理:

定理 1 (“石头剪刀布”定理):如果剔除“平局”不考虑(即,忽略甲乙双方都出相同手势的情况),那么,

(1)针对甲方来说,对任意 $k/n\leqslant C$,都一定有某种技巧(对应于仙农编码),使得,在 nC 次游戏中,甲方能够胜乙方 k 次;如果在某 m 次游戏中,甲方已经胜出乙方 u 次,那么,一定有 $u\leqslant mC$。这里 C 是“甲方信道”的容量。

(2)针对乙方来说,对任意 $k/n\leqslant D$,都一定有某种技巧(对应于仙农编码),使得,在 nD 次游戏中,乙方能够胜甲方 k 次;如果在某 m 次游戏中,乙方已经胜出甲方 u 次,那么,一定有 $u\leqslant mD$。这里 D 是“乙方信道”的容量。

(3)如果 $C<D$,那么,整体上甲方会输;如果 $C>D$,那么,整体上甲方会赢;如果 $C=D$,那么,甲乙双方势均力敌。

由于“甲方信道”和“乙方信道”的信道容量都有现成的计算公式,为避免喧宾夺主,更为了不少读者朋友被过多的数学公式吓跑,我们就在些略去 C 和 D 的计算细节了(有特殊兴趣的读者,可见附件中的 Word 版本)。

2 巧胜策略

根据定理 1,可知,甲乙双方在“石头剪刀布”游戏中的胜负,其实已经事先就“天定”了,某方若想争取更大的胜利,那么,他就必须努力“改变命运”。下面分几种情况来考虑:

2.1 两个傻瓜之间的游戏

所谓“两个傻瓜”,意指甲乙双方都固守自己的习惯,无论过去的输赢情况怎样,他们都按既定习惯“出牌”。这时,从定理 1,我们已经知道:如果 $C<D$,那么,整体上甲方会输;如果 $C>D$,那么,整体上甲方会赢;如果 $C=D$,那么,甲乙双方势均力敌。

2.2 一个傻瓜与一个智者之间的游戏

如果甲是傻瓜,他仍然坚持其固有的习惯“出牌”,那么,双方对抗足够多的次数后,乙方就可以计算出对应于甲方的,随机变量 X 的分布概率 p 和 q,以及相关的条件概率分布,并最终计算出“甲方信道”的信道容量,然后,再通过调整自己的习惯(即,随机变量 Y 的概率分布和相应的条件概率分布等),最终增大自己的“乙方信道”的信道容量,从而,使得后续的游戏对自己更有利;甚至使“乙方信道”的信道容量大于“甲方信道”的信道容量,最终使得自己稳操胜券。

2.3 两个智者之间的游戏

如果甲和乙双方,都随时在总结对方的习惯,并对自己的“出牌”习惯做调整,即,增大自己的信道容量。那么,最终,甲乙双方的“信道容量”值将趋于相等,即,他们之间的游戏竞争将趋于平衡,达到动态稳定的状态。

3 简化版本

虽然上面几节,完美地解决了“石头剪刀布”游戏

问题,但是,它们在保持“直观形象”的优势下,付出了“复杂”的代价。下面,我们再给出一个更抽象,更简捷的解决办法。

设甲与乙玩“石头剪刀布”。他们可分别用随机变量 X 和 Y 来表示:

当甲出拳为剪刀、石头、布时,分别记为 $X=0$、$X=1$、$X=2$;

当乙出拳为剪刀、石头、布时,分别记为 $Y=0$、$Y=1$、$Y=2$。

根据概率论中的“大数定律”,频率的极限趋于概率,所以甲乙双方的出拳习惯,可以用随机变量 X 和 Y 的概率分布表示为:

$0<P_r(X=x)=p_x<1, x=0,1,2, p_0+p_1+p_2=1$;

$0<P_r(Y=y)=q_y<1, y=0,1,2, q_0+q_1+q_2=1$;

$0<P_r(X=x,Y=y)=t_{xy}<1, x,y=0,1,2, \sum_{0\leqslant x,y\leqslant 2}t_{xy}=1$;

$p_x=\sum_{0\leqslant y\leqslant 2}t_{xy}, x=0,1,2$;

$q_y \sum_{0\leqslant x\leqslant 2}t_{xy}, y=0,1,2$。

“石头剪刀布”游戏的输赢规则是:若 $X=x, Y=y$,那么,甲(X)赢的充分必要条件是:$(y-x)\bmod 3=2$。

现在构造另一个随机变量 $F=(Y-2)\bmod 3$。考虑由 X 和 F 构成的信道($X;F$),即,以 X 为输入,以 F 为输出的信道。那么,就有如下事件等式:

若在某个回合中,甲(X)赢了,那么,就有($Y-X$)$\bmod 3=2$,从而,$F=(Y-2)\bmod 3=[(2+X)-X]\bmod 3=X$,也就是说:信道($X;F$)的输入($X$)始终等于它的输出($F$)。换句话说,1 个比特就被成功地在该信道中被从发端传输到了收端。

反过来,如果“1 个比特就被成功地在该信道中被从发端传输到了收端”,那么,就意味着“信道($X;F$)的输入(X)始终等于它的输出(F)”,也就是说:$F=(Y-2)\bmod 3=X$,这刚好就是 X 赢的充分必要条件。

结合上述正反两个方面的论述,就有:甲(X)赢一次,就意味着信道($X;F$)成功地把 1 比特信息,从发端送到了收端;反之亦然。因此,信道($X;F$)也可以扮演第三节中“甲方信道”的功能。

类似地,若记随机变量 $G=(X-2)\bmod 3$,那么,信道($Y;G$)就可以扮演前面“乙方信道”的角色。

而现在信道($X;F$)和($Y;G$)的信道容量的形式会更简捷,它们分别是:

($X;F$)的信道容量 $=\mathrm{Max}_X[I(X,F)]=\mathrm{Max}_X[I(X,(Y-2)\bmod 3)]=\mathrm{Max}_X[I(X,Y)]=\mathrm{Max}_X[\sum t_{xy}\log(t_{xy}/(p_xq_y))]$,这里的最大值,是针对所有可能的 t_{xy} 和 p_x 而取的,所以,它实际上是 q_0, q_1, q_2 的函数。

同理,($Y;G$)的信道容量 $=\mathrm{Max}_Y[I(Y,G)]=\mathrm{Max}_Y[I(Y,(X-2)\bmod 3)]=\mathrm{Max}_Y[I(X,Y)]=\mathrm{Max}_Y[\sum t_{xy}\log(t_{xy}/(p_xq_y))]$,这里的最大值,是针对所有可能的 t_{xy} 和 q_y 而取的,所以,它实际上是 p_0, p_1, p_2 的函数。

其他讨论就与上面几节相同的,不再重复了。

4　结束语

“攻防”是安全的核心,所以,在建立“安全通论”的过程中,多花一些精力去深入研究“攻防”也是值得的。

在文献[2]中,我们研究了“安全通论”的盲对抗问题,本文研究的“石头剪刀布”游戏则是一种“非盲对抗”,但由于它的普及率极高(几千年来,全世界每个人在童年时代几乎都玩过),所以,我们以单独一篇论文的形式来研究它。有关其他一些有代表性的“非盲对抗”,我们将在随后的文章中研究。

当然,换一个角度来看,也可以说:我们的“安全通论”虽然刚刚诞生,它就大显身手,成功地扫清了古老“石头剪刀布”游戏中的若干迷雾。所以,“安全通论”确定大有前途。

参考文献:

[1] 杨义先,钮心忻. 安全通论(1)之“经络篇”[EB/OL]. http://blog.sciencenet.cn/blog-453322-944217.html,2015-12-18.

[2] 杨义先,钮心忻. 安全通论(2):攻防篇之“盲对抗”[EB/OL]. http://blog.sciencenet.cn/blog-453322-947304.html,2016-01-01.

[3] Thomas M Cover, Joy A Thomas. 信息论基础[M]. 阮吉寿,张华,译. 北京:机械工业出版社出版,2007.

[4] Shu Lin, Daniel J, Costello Jr. 差错控制码[M]. 晏坚,何元智,潘亚汉,等译. 北京:机械工程出版社,2007.