THE ADVENT OF CRYPTOLOGY IN THE GAME OF BRIDGE

PETER WINKLER

ABSTRACT: The surprising discovery that information can be passed both covertly and legally between bridge partners has added a new dimension to the theory of this popular game. In this paper some of the methods are sketched and their cryptologic foundation is described.

KEYWORDS: Cryptology, bridge.

The recent introduction of cryptologic techniques into bidding and defense in bridge has generated interest and controversy on both sides of the Atlantic, and threatens to add a significant new dimension to the theory of the game. We believe this development to be of interest to the cryptologic community, partly because there are some interesting aspects concerning the creation of key from partial information, but also because there is a possibility that some fraction of the large number of serious bridge players may, as a result, become interested in cryptology.

Of the three major activities--bidding, defense and dummy play--that comprise the game of bridge, the first two require cooperation between partners. It is thus desirable in both cases to communicate as much information as possible to one's partner, while giving as little as possible to the opponents. This procedure is made difficult to achieve by two laws of the game: (1) all communication must be done via legal calls and card plays; and (2) partnerships may not have private agreements (e.g., about the meaning of some call or play.)

It is thus not surprising that, until recently, secret communication with one's partner was generally regarded as solely the province of cheaters. Ethical bridge players concentrated on communicating whatever information seemed to be more likely to help partner than the opponents. In doing this they are permitted to have prior agreements--possibly of very complex and artificial nature--between partners, but all such agreements must be revealed in advance to the opponents.

Suppose, for example, that in the course of bidding toward a slam South wishes to tell his partner (North) that he holds the ace of clubs. He can usually do this by making some appropriate call (e.g. a cue-bid of Four Clubs) but the opponents may also benefit from this information, particularly in the selection of opening lead. For South instead to write a note and pass it under the table to North would obviously be a violation of law (1). Alternatively, the North-South partnership might have an understanding that in the present auction a bid of Four Hearts shows the ace of clubs; but then law (2) requires that the agreement be made known in advance to the opponents.

Nonetheless, the information that South has the ace of clubs is sometimes passed to North in covert but legal fashion. If North, holding the other three aces, were to employ some ace-asking convention (such as Blackwood) and receive a one-ace reply, he would know of course that his partner's ace is in clubs; but no law requires North to reveal to the opponents what he can deduce from looking at his own hand. This instance is of little practical importance, since when North-South hold all the aces the opponents are not likely to care who holds which.

On the other hand, once one piece of information has been passed covertly it can be used as key for another: thus, conceivably, South's next bid might carry the message "I hold the king of the suit in which I hold the ace."

The following example is intended to reduce the situation to its simplest cryptographic terms. Suppose each of three people, A, B and C, is dealt a random card from a deck consisting only of the three cards x, y and z. A wishes to convey a single bit of information (e.g., whether or not he dyes his hair) to B but not to C, in the presence of both. If A holds x and "guesses" that B holds y, he can make the following announcement: "I hold either x or y." If B responds "so do I," then key is established. If A dyes his hair then he can now say "I dye my hair if my card is x, otherwise I do not." C remains in the dark.

On the other hand if A misguesses (B holds z, not y) B will respond "Sorry; I have neither x nor y;" the key is now blown and A cannot attain his objective. If we define a bit of key to be sufficient for covert communication of a single binary piece of information, then it appears that in this example A has access to, on the average, half a bit of key. Note, by the way, that if C had for some reason revealed his holding, no guessing by A would have been necessary.

With four people dealt thirteen cards each, A could make thirteen guesses of the sort described above, each with success probability one-third (since B has 13 of 39 outstanding cards); hence an average of at least 13/3 bits of key

seems available for covert partnership communication. This is not much to a cryptographer, who needs 23 bits of key to encrypt a telephone number, but to a bridge player the ability to transfer even a single bit of information covertly could be crucial.

Of course, the guessing needed to establish key at the bridge table has to be coded into legal calls. Since there are barely enough of these for sufficient communication to arrive at a good contract, they cannot be wasted solely on the establishment of key. Hence we attempt to establish key only when the attempt simultaneously passes information valuable in the selection of a contract. Key obtained in this manner will be termed active key.

When the opponents have the strong hands we must often be content to listen; frequently their bidding will reveal a piece of information which can be used to establish our key "for free." This passive key can then be used to encrypt defensive signals.

Here is a simple example of an active crypto-convention. A jump raise of partner's opening suit traditionally shows a strong hand with trump support; suppose we require, additionally, either the ace or king of trumps. (With both or neither, some other response, e.g. 3NT, can be employed.) This is useful in itself, since trump quality is important in slam bidding, but it is also an attempt to establish key. If opener is missing both top trumps, he rebids (say) 3NT and key is lost; but otherwise, if interested in slam, he does the following: with the ace of trumps he cue-bids normally, but with the king of trumps he cue-bids a suit in which he lacks control. Responder can tell which by looking at his own top trump, but the opponents have not been tipped off as to the killing opening lead. This could be especially important in duplicate bridge where overtricks are often crucial.

Certain modern conventions which guarantee specific holdings make key establishment an easy second step. An example is "disciplined" weak two-bids, in which an opening two-bid in first or second position shows two of the top three honors in the named suit. Why not have some response (say 2NT) guarantee the missing honor? This could provide a three-way encryption of openers "feature" rebid. Thus the sequence 2 Spades—2NT—3 Hearts could show "either AK of spades and a high heart or AQ of spades and a high diamond or KQ of spades and a high club." Only partner knows for sure!

A variation of a convention sometimes called "Rosenkranz" enables the partner of the overcaller to show the A or K of the overcaller's suit (to indicate a safe lead). Add a way for overcaller to confirm the other card and a scheme for utilizing the key, and "Rosenkranz" becomes "Rosencrypt".

To take advantage of passive key one needs at least two different opening lead agreements (e.g. "fourth best" and "third/fifth") and at least two signalling systems (e.g. "low card encourages" and "high card encourages"). One of the systems is selected for default use when no key is obtained.

Key is obtainable whenever the opponent who eventually becomes declarer gives a reliable count of some quantity in his hand. Examples: declarer answers the Stayman convention, showing four cards of a certain suit, or used the splinter convention, showing one card; declarer shows his aces and kings in a Blackwood reply; declarer reveals his high-card point count within close limits in a notrump sequence; declarer shows out of a suit early in the play. In each case the exposure of the dummy will enable each defender to count the number of the objects in question held by his partner; this becomes key. The opening leader can, for example, use one lead agreement when holding an odd number of "objects" and the other when holding an even number. Partner can "read" the lead as soon as dummy is spread, but hopefully the declarer cannot, until too late in the play.

When key is obtained because declarer has shown out of a suit, it is too late to encrypt the opening lead but perhaps not too late to encrypt some defensive signals. Here a fancy encryption scheme can be used because the defenders may have a lot of reliable key: they, and the only they, know the exact spot-card distribution of the suit in question.

In the following example, taken from [4], East is dealer and neither side is vulnerable.

North
S: 652
H: 1085
D: 74
C: KQJ105

West	East
S: 983	S: QJ4
H: QJ962	H: AK73
D: 1083	D: 952
C: 92	C: A74

South
S: AK107
H: 4
D: AKQJ6
C: 863

East	South	West	North
1NT*	DBL	2H	Pass
Pass	3H	Pass	4C
Pass	4D	Pass	5D(end)

*12-14 points

Playing standard leads and defensive signals, West leads the queen of hearts; declarer ruffs the continuation, draws trumps, and plays the three of clubs toward the table. West is stymied.

If he plays the club deuce, East will think he has three cards in the suit and will win the second round; declarer will take the rest. But if West signals honestly to partner with the nine, declarer will see that he cannot flush out East's ace in two rounds and will be forced to use his club entries to take the double finesse in spades, a play West knows will win.

Playing encrypted signals as described in [2], West has a way out. Hearts, the suit in which declarer has shown out, has become "key" and after trick two declarer cannot tell whether defenders are using normal or upside-down signals. West signals honestly to his partner and declarer must guess.

It should be noted that although passive key is more easily obtained than active key, it must be used with discretion. Some forms are not completely reliable (e.g. Stayman, point-count). Opening leads can be blown and repeated defensive signals present declarer with depths. Worse, it may occasionally happen that the key can be "turned"--declarer determines during the play what system is in use, and takes advantage of deductions concerning the location of cards involved in the key. On balance, though, most forms of passive key are safe and effective. The author leads "attitude" against 3NT with 7 or more points, but fourth-best with 6 or fewer; even though partner cannot always read the lead and declarer can theoretically profit in some circumstances, this convention seems to work nicely.

What is the future of cryptology in bridge? Alan Truscott, bridge columnist of the New York Times, predicted in [1] that it would "open an entirely new field in bridge theory." Further articles [3], [4] and [5] have suggested a variety of other conventions, and we refer readers to these for details. Encryption is already in use by the Taiwanese international bridge team, and is beginning to crop up occasionally in team play. On the other hand, it will be a while before cryptologic conventions are permitted in ordinary tournament play; one such convention was recently turned down in Great Britain, prompting

a scathing editorial in Bridge Magazine. Moreover, all uses of encryption found so far have limited application below the expert level.

As players get better, however, and bidding systems become more accurate, the need for encryption grows; and many more uses for cryptology in bridge may yet be found.

REFERENCES

1. Truscott. Odd Signal Switch. New York Times, Sunday, July 13, 1980.

2. Winkler, P. 1980. Encrypted Signalling. The Bridge World. April: 25-26.

3. Winkler, P. 1980. Knockout. The Bridge World. December: 18-22.

4. Winkler, P. 1981. Cryptologic Techniques in Bidding and Defense, Parts I, II, III, and IV. Bridge Magazine. April: 148-149, May: 186-187, June: 226-227, and July: 12-13.

5. Winkler, P. 1981. My Night at the Cryppie Club. Bridge Magazine. August: 60-63.

Almanac

Friday, May 6, 1983
126th day; 239 to go this year
Sunrise: 5:56; Sunset: 8:24

Today's weather

East wind, rain

TALK ABOUT MISROUTED AND DELAYED MESSAGES!