Bridge Cryptography Fundamentals

JOHN L. SIMONS

Abstract  Cryptography requires a priori key transfer over a private channel to facilitate the exchange of coded messages over a public channel. In the game of bridge, all bidding and card playing is public information for all four players. However, under special conditions it is possible to define a key exclusively between partners. This key can subsequently be used to transfer coded bids and cards. Cryptography in bridge was introduced by Winkler [6]. We derive a lemma that explains the conditions for key transfer under the rules of bridge. Some examples will be given. Very elementary understanding of bridge and cryptography suffices to understand the fundamentals of bridge cryptography.

Keywords  bridge cryptography, coded bidding, coded playing, information use, rules of bridge

Introduction

Bridge is a card game for two teams of two players. Each player receives 13 cards at random during the deal. The two teams compete in two successive phases of the game. During bidding the players take part in an auction of increasing bids to define a contract (number of tricks of a total of 13) for which a team is willing to play. During playing one of the players (usually called South) becomes the declarer. His companion (North) becomes dummy and his cards are shown to all players after West (one of the two opponents West and East) has chosen an opening lead. If the declarer wins at least the amount of tricks they agreed on, he wins his contract and his team earns credit points. If he does not succeed, the contract is defeated and the opponents earn credit points.

Bridge probably originated from an older card game named whist around 1920. During the years bridge has become more and more scientifically based. Not only bidding and playing are dominated by conventions (which give a specific meaning to a bid or a played card), also probability calculus for choosing a line of play is used by almost all players [2]. Top players optimize their bidding and playing (signalling) conventions in the sense that the information transfer between partners is optimized. It is strictly against the rules to use any other information than the bids and played cards and all information that is transferred between partners must be freely available for the opponents. To prevent illegal information transfer between partners (e.g., thinking time, body language) bidding screens are diagonally placed on the bridge table in international tournaments.

In the game of bridge (and other games [4]) the situation around key transfer is somewhat different from standard cryptography, because the rules of bridge require
that the bidding (e.g., Acol and Precison systems) and playing (e.g., Lavinthal and Journalist signalling) conventions are made public before playing. So there is no private channel for key transfer. Sometimes partners can, however, exchange information about the cards in their hands over the public channel, which only they can interpret. Take as an example the situation during playing where the declarer shows a void and West and East have not yet shown a void in a suit. Consequently they (and only they) know which one has the highest card in that suit and they can use that common information to encipher and decipher signalling. So West and East firstly build (or define) a key because the conditions allow them to do so. After this key has been established it can be used for enciphering and deciphering coded cards. The declarer may try to break the code during the further course of the game.

Definitions of Bridge Cryptography

Consider the set $S$: the complete deck of 52 bridge cards. Let $S_i$ and $S_j$ be disjoint subsets of $S$ and let $S_k = S_i \cup S_j$. Let $m_i$ be a measure defined for any subset $S_i$ for which $m_k = m_i + m_j$ and $m(S) = M$. Some examples of such measures are

1. The number of high card points HCP (Ace = 4, King = 3, Queen = 2, Jack = 1), $M = 40$.
2. The number of aces, $M = 4$.
3. The number of honor cards (AKQJT), $M = 20$.
4. The number of cards in a given suit, $M = 13$.

In bridge several other relevant concepts, that do not satisfy the measure condition for disjoint sets, exist to guide bidding and playing.

- The classic first controls in a suit (ace and void). If one hand (subset) has the ace in a suit then another hand (disjoint subset) can have a void in that suit. The combined hands only have the ace.
- The number of different colors. Each hand can have 1 up to 4 different colors, while the total number of colors is 4.
- The number of potential playing tricks. An $AKQxxx$ combination in a particular hand represents 6 potential tricks. The total number of playing tricks of the deck is 52.
- The losing tricks count. Combinations like $Axx$, $Kxx$, $Qxx$ count for 2 losing tricks in that suit. The number of losing tricks heavily depends on the actual distribution of the cards, while the number of losing tricks of the deck is zero!
- The total number of tricks. The law of total tricks was introduced in 1969 by Jean Vernes in Bridgeworld. It states that the sum of tricks for North-South and East-West is equal to their sum of trumps in their longest suit [1] and has been questioned since then. This concept produces a special case because the measure condition holds for the combination of partners hands and does not hold for other subsets!

Measures as well as non-measures form the basics of many bidding and playing tactics. High card points are widely used in modern bidding systems like Acol for an opening bid, playing tricks were used in the past, the losing trick count [3] is used to determine the level of a contract, and the law of the total number of tricks is often used in competitive bidding situations.
Now consider two disjoint subsets $S_{NS}$ (the combined hands of N and S) and $S_{EW}$ (the combined hands of E and W). When in a phase of a bridge game the value of a measure for the subset defined by the combined hands of the opponents is approximately known by both partners, then also the value of the measure of the combined hands of partners is approximately known. If one of the partners is able (by bidding or playing) to define two disjoint intervals for the value of the measure of his hand then also the other partner can approximately define two disjoint intervals for the value for the measure of his hand. Then both partners (and not the opponents) can identify which of the two interval pairs applies.

A Cryptographic Bridge Lemma

This intuitive notion can be made formal by the following. **Lemma.** Let $m$ be a measure defined for any subset of $S$ ($S$ is the complete card deck with $m(S) = M$). Let $m_N$, $m_E$, $m_S$, and $m_W$ be the measures of the hands of the four bridge players. Suppose that at a stage in the game all players know that

\[
m_1 \leq m_N + m_S \leq m_1 + d_1
\]

and know that either $m_W \leq m_2$ or $m_W > m_2 + d_2$ with $d_2 \geq d_1 \geq 0$ (where $m_1$, $m_2$, $d_1$, and $d_2$ may be defined either prior to the actual game or via prior information exchange such as leading cards during the game). Under these assumptions all players know that either

\[
\begin{align*}
m_W &\leq m_2 \\
m_E &\geq M - m_1 - m_2 - d_1
\end{align*}
\]

or

\[
\begin{align*}
m_W &> m_2 + d_2 \\
m_E &< M - m_1 - m_2 - d_2.
\end{align*}
\]

*Only West and East know which of these two possibilities applies.*

**Proof.** Because

\[
M = m_N + m_E + m_S + m_W
\]

one has

\[
M - m_1 - d_1 \leq m_E + m_W \leq M - m_1.
\]

If $m_W \leq m_2$ then $m_E \geq M - m_1 - d_1 - m_W \geq M - m_1 - m_2 - d_1$ and vice versa. If $m_W > m_2 + d_2$ then $m_E \leq M - m_1 - m_W < M - m_1 - m_2 - d_2$ and vice versa. West knows which of the two possibilities $m_W \leq m_2$ and $m_W > m_2 + d_2$ actually exists and equally East knows which of the two possibilities $m_E \geq M - m_1 - m_2 - d_1$ and $m_E < M - m_1 - m_2 - d_2$ actually exists. So both players know which of the two original possibilities either (2) or (3) applies.

Winkler [6] distinguishes active key definition where East and West themselves establish equation (5) and passive key definition where the opponents North and South establish equation (1). In our terms Winkler implicitly assumes $d_2 = d_1 = 0$ for active keys and $d_2 = d_1 \geq 0$ for passive keys, which is sufficient, however not
necessary, for key transfer. From the measure requirement equation (4) it follows that there is no theoretical difference between active and passive key definition. For both cases the necessary requirement is $d_2 \geq d_1 \geq 0$.

**Applications of Cryptography (Cryptotechniques) in Bridge**

The next example is an adaptation of an example of Winkler.

**Cryptotechnique During Playing**

Suppose that West and East have agreed on the following leadconvention: $A$, $T$ or 9 lead against No Trump shows

- Either 4 cards in the suit with at most 7 HCP. In this case the lead player (West) signals low cards as positive and East signals high cards as positive.
- Or 5 cards in the suit with at least 10 HCP. In this case the lead player (West) signals high cards as positive and East signals low cards as positive.

This agreement is known to the opponents North and South as well. After the bidding 1NT, 2NT, 3NT, West leads the T of spades in the following game

```
North  ♠872
       ♦82
       ♣K94
       ♠AQT96

South  ♠AJ4
       ♦AJ9
       ♣AQ76
       ♥853
```

When dummy opens, East can (based on his own hand and under the assumption of an opening bid of South with 15 – 17 HCP) calculate which of the two possibilities for West (either at most 7 HCP or at least 10 HCP) applies. North plays low, East plays the Q of spades, and South must choose one of two possibilities:

- If West has at least 10 HCP and 5 spades, then East has a 2 spades. Now the declarer is likely to lose 4 spade tricks if the cards lay as follows:

```
West  East
♠KT963  ♠Q5
♥Q743  ♥7653
♦J8  ♦T32
♥J4  ♥K72
```

- If West has at most 7 HCP and 4 spades, then South can afford to loose three spade tricks. The cards may lay as follows:

```
West  East
♠KT96  ♠Q53
♥Q74  ♥K7653
♦T852  ♦J3
♥J4  ♥K72
```
The crucial difference in knowledge is that all South can do is make a hypothetical judgement, whereas East knows which of the two possibilities actually exists. If South goes up and takes the club finesse then the contract is defeated if the first case applies. If South ducks then East may switch to hearts and the contract is almost certainly defeated if the second case applies. South can disperse noise in the communication channel by sometimes bidding 1NT with 14 or 18 high card points and this is indeed what good bridge players do anyway.

**Cryptotechnique During Bidding**

There are many conventions for slam bidding. The well-known Blackwood convention (or variants like Roman Key Card Blackwood) are used to discover the number of aces (or key cards) held by the bidder’s partner. In the standard version of Blackwood, a player bids 4NT, which asks his partner to bid 5 clubs with 0 (or 4) aces, 5 diamonds with 1 ace, 5 hearts with 2 aces, or 5 spades with 3 aces. Many players only use such conventions if they possess at least one ace. In that case, an alternative answering scheme can be based on a cryptotechnique, where the asking bid 4NT has the following answers:

- $5\spadesuit$ means 0 or 1 ace
- $5\heartsuit$ means $\heartsuit A + \spadesuit A$ or $\spadesuit A + \clubsuit A$
- $5\diamondsuit$ means $\diamondsuit A + \clubsuit A$ or $\spadesuit A + \heartsuit A$
- $5\clubsuit$ means $\clubsuit A + \clubsuit A$ or $\spadesuit A + \heartsuit A$
- $5NT$ means 3 aces

In case of two aces in the answering hand, both partners know which of the two alternatives applies. If one of the opponents has the fourth ace, then he also has this key and can break the code. Thus this mutual knowledge cannot always be used as a key for further coded bidding. In case of three aces in the answering hand both partners and no opponent has a key for further coded bidding.

**Consequences of Cryptography in the Game of Bridge**

- Barriers for cryptotechnique during bidding. A popular bidding convention is a multicolor opening bid. A multicolor bid defines two approximately specified intervals for one of the defined measures, and therefore complicates the counter action of opponent’s bidding system if it is based on knowledge of such a measure. Some common multicolor bids are widely accepted (e.g., $2\diamondsuit$) whereas other similar bids (e.g., $3\spadesuit$) are forbidden in the practice of bridge tournaments. The argument given by tournament directors is the unbalance of information.
- Cryptotechnique and the laws of bridge. The official rules of the international bridge federation use the word *information* when describing what is accepted during bidding and play without making a clear distinction about the source of the information being the system and/or the actual cards. Law 16 reads... *Players are authorized to base their calls and plays on information from legal calls and or plays, and from mannerisms of opponents. To base a call or play on other extraneous information may be an infractions of law.* Law 75 reads... *Special partnership agreements, whether explicit or implicit, must be fully and freely available to the opponents. Information conveyed to partner through such agreements must arise*
from the calls, plays and conditions of the current deal [5]. As a result cryptographic techniques are sometimes forbidden in tournaments based on an interpretation of the rules by the arbiter, although the rules allow them.

- Cryptotechnique and information processing capacity. Chinese bridge teams have experimented with cryptographic signalling. In general these techniques have not received much attention in tournament practice. One reason are the laws of bridge but another important reason is the extra load on the information processing capacity of players. For computer bridge this last argument does not hold and it can be conjectured that advanced bridge software will include cryptographic techniques in the future. Then computer bridge as a game starts to diverge from human bridge, just as has been the case in chess.

About the Author

John Simons received his Masters degree in system engineering and Ph.D. in applied number theory from Delft University of Technology. From 1971 to 1988 he worked as a research engineer and systems analyst in aeronautics, telecommunications, and agriculture. Since 1988 he has been a full professor in industrial engineering at the University of Groningen in the Netherlands. His (research) interests are industrial mathematics and applied number theory. John Simons is a member of the European Mathematical Society and the Mathematical Association of America.

References