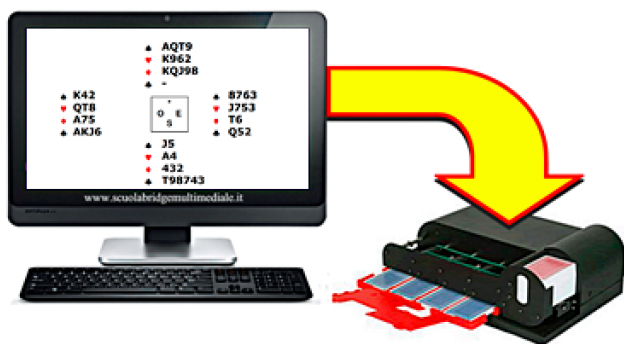


Il percorso delle mani computerizzate e il generatore SquareDeal

Il generatore BigDeal

Oramai da circa un ventennio in tutti campionati nazionali e internazionali si utilizzano le mani elaborate dal computer. In meno di un secondo, grazie a software dedicati, si elaborano set di smazzate - salvate in un unico file - necessarie alla varie competizioni. In commercio vi sono numerosi generatori di smazzate, quello oggi più utilizzato e divenuto standard mondiale è il BigDeal, ideato dall'olandese Hans van Staveren. EBL,WBF lo usano dal 2000, FIGB qualche anno dopo, e dal 2017 anche da ACBL (Usa).



Smazzatrice Duplimate-MK-IV

La smazzatrice, collegata a un PC, legge il diagramma della mano elaborato dal PC e riempie il board in circa 5 -7 secondi. Le macchinette, sempre più veloci e affidabili, possono preparare sino a 600 boards/ora.

Il BigDeal, a differenza di altri generatori, produce le smazzate "prelevandole", dalla propria banca dati interna, **non prevede né consente alcuna possibilità d'intervento manuale** da parte dell'operatore. E fin qui *non vi possono sussistere dubbi*.

Dati statistici

Tutti i generatori di smazzate distribuiscono equamente, per default, con lievi variazioni in percentuale, i punti onori tra le quattro posizioni: Nord, Est, Sud e Ovest. Ciò è facilmente verificabile, poiché gli stessi software sono in grado di analizzare le mani da loro elaborate e di fornirvi il relativo prospetto statistico: vuoti, singoli, colori lunghi ecc.. Chi sostiene che una linea viene agevolata dalla solita malvagia manina federale può tranquillamente estrarre il prospetto statistico di seguito indicato.

Hands Statistics:

Hand:	N	S	E	W	NS	EW
Average HCP:	9,97	10,07	10,27	9,70	20,03	19,97
Balanced:	15	14	16	11	29	27
Voids:	0	0	1	2	0	3
Singletons:	12	12	8	13	24	21
Long suits (7+):	0	0	2	1	0	3

Il prospetto che indica frequenza e distribuzione delle mani elaborate. HCP = Media Punti Onori

I bridgisti meno esperti non amano le mani computerizzate. Basta chiamare uno slam e trovare due Re secchi fuori impasse per creare irritazione nel giocatore, stramaledire le mani computerizzate e prendersela con la solita dispettosa manina, che ripeto, di fatto, non c'è. Se un Re secco è nelle mani mescolate al tavolo, tutti in silenzio.

Il file originario di "x" mani prodotto dal BigDeal può essere tuttavia successivamente manipolato dall'organizzatore del torneo. In rete sono disponibili gratuitamente software che consentano l'edizione, mano per mano, in genere a uso didattico. Fare queste variazioni su di un file di gara sinceramente è da maniaci fancazzisti. Ma chi si mette a editare le mani e spostare gli onori a destra e a manca, e poi a quale scopo?

Diverso il discorso di come rendere più vivaci le varie competizioni, specie nelle fasi finali. In molti giocatori è maturata la convinzione che le smazzate non siano del tutto casuali e che qualche abile manina effettui una sorta di "pettinatura" eliminando le smazzate insignificanti, e che nelle finali trasmesse da BBO, a mo' di "spettacularizzazione", addirittura inserendo qualche slam in più oltre la media.

Bisogna riconoscere che una finale di campionato e/o competizione internazionale con mani piatte non soddisfa più nessuno, idem un mitchell locale giocato con carte vecchie, spesse, grandi e scarsamente mescolate (alla vecchia maniera per intenderci).

Segnalo che una sorta di "filtro", gestito via software, è applicato dalla maggioranza dei siti che offrono il bridge online. Giocare a tarda notte un duplicato di otto mani con un "passo" e cinque o sei parzialini... beh, meglio andare a letto a dormire.

Esempio di manipolazione

Chiedo a BigDeal di elaborare 30 mani, le analizzo con un software adatto a definire i “Contratti Realizzabili”, poi seleziono solo venti mani (il requisito) a mio piacimento e infine salvo il file da mettere in pista. Un lavoretto di due minuti che chiunque può fare. Ecco un classico esempio di taroccamento del file generato da BigDeal.

Critiche ai Responsabili gare

Gli organizzatori o, più precisamente, i Responsabili tecnici incaricati di fornire il file delle mani ai duplicatori, a torto o a ragione, in questi anni hanno dovuto subire numerose critiche da più parti del mondo, Italia inclusa, senza tuttavia essere in grado di dimostrare un bel nulla e, fortunatamente per loro, manco i sospettosi utenti finali.

Nuovo Software

Per ovviare in parte a quanto sopra, l'ideatore del BigDeal ha ora realizzato un nuovo software denominato SquareDeal. Tale programma elabora le smazzate come in precedenza ma in aggiunta richiede l'inserimento di parametri identificativi e codici vari affinché l'organizzatore possa finalmente dimostrare agli utenti finali che il file delle mani in uso corrisponde, in tutto per tutto, all'originale. Verifiche in tal senso possono essere effettuate dai partecipanti ai tornei. Beh, è già qualcosa.

Dettagli tecnici sul nuovo software con relativa procedura - emessa anche da WBF - valida sia per gli organizzatori sia per i (sospettosi) giocatori sono ampiamente descritte in allegato.

L'implementazione del BigDeal in SquareDeal serve anche a Staveren. Ora nessuno potrà scaricare su di lui colpe sulla configurazione e frequenza di certe smazzate.

Un passo avanti, ma non basta...

Indubbiamente la garanzia di avere un file non manomesso è un passo avanti, tuttavia, ancora nulla impedisce all'organizzatore, o alla stanza di duplicazione, di divulgare e/o vendere in anticipo i record delle mani a determinati giocatori.

Sapete chi ha scritto questa bella noticina?
Lo stesso **Hans van Staveren**.

Operare in regime di sicurezza

Diciamo grazie a Staveren, ma il vero problema delle mani computerizzate è mantenerle segrete durante l'intero percorso successivo all'elaborazione: dalla fase di duplicazione sino alla consegna del file agli operatori di BBO, altro punto critico.

Le dimensioni del file, molto ridotte - da 2 a 6 KB -, non creano problemi, facile da copiare su chiavetta USB in due secondi, sia il file che i diagrammi delle mani possono

essere inviati via e-mail, agli smartphones, ecc...

A livello più spinto basterebbe anche una banalissima microcamera per filmare le mani che girano sul monitor in sala duplicazione. Le vie del Signore sono infinite.



Operatori BBO

A pensare male si fa peccato... (cit. Andreotti).

Alcuni operatori di BBO lavorano con il loro PC, con un software pre-installato in pochi secondi possono determinare i Contratti Realizzabili di tutte le mani del segmento di gara.

Domanda: quanto tempo prima dell'evento viene consegnato il file delle mani agli operatori BBO?

Anche comunicazioni last-minute sono possibili. E' sufficiente un banalissimo segnale per comunicare all'amico seduto al tavolo se nella mano in corso c'è slam o no (*sarà il caso di mettere un sipario tra l'operatore e il tavolo con vetro riflettente da un lato e trasparente dall'altro*).

Nelle competizioni internazionali tra sala Aperta e Chiusa, gli operatori BBO sono tanti, volendo una talpa si trova sempre. La WBF ha adottato un apposito protocollo di sicurezza.

Le contromisure della World Bridge Federation (WBF)

Ecco cosa ha risposto Maurizio Di Sacco, responsabile presso la WBF, in un post di facebook:

12 marzo 2018

Domanda: I duplicatori vedono le mani e chi consegna il file delle mani agli operatori di BBO? E quando tempo prima dell'evento?

Risposta: I duplicatori vedono le mani, gli operatori BBO no, perché non ricevono il file (a livello internazionale, dico) perché il protocollo di sicurezza da me fissato alla fine del 2007 prevede l'utilizzo di uno speciale software (che la FIGB non ha) che rilascia le mani una, ad una.

Dove ci sono io (EBL, WBF, CAC e CBS) la procedura è scritta e obbligatoria. Te la posso spiegare facilmente: le mani vengono prodotte da me, in un computer che non è mai collegato ad internet, e poi stoccate in una chiavetta USB che io porto sempre con me, e che è criptata. Subito prima dell'inizio del campionato, le mani vengono inserite nel server di gestione, in un'area ad altissimo livello di encrypting (secondo i nostri esperti, violare il file è quasi impossibile, e comunque richiederebbe mesi ad un hacker formidabile). Da lì, vengono rilasciate una ad una a BBO secondo il seguente principio: l'operatore riceve una nuova mano solo dopo che ha comunicato il

risultato della precedente.

Anche per quanto riguarda la pubblicazione su internet dei risultati, una mano diventa visibile (ovvero viene appositamente rilanciata dal server) solo quando il server ha ricevuto il relativo risultato da tutti i tavoli.

L'unico anello debole della catena è la duplicazione, ma il nostro gruppo è di eccezionale affidabilità. Inoltre, la sala duplicazione è isolata da internet (non è mai cablata, ed i computer usati hanno la connessione wireless non utilizzabile). Dal 2009, è anche video sorvegliata.

P.S.:

Il watch apple è vietato, così come ogni apparato che può trasmettere e/o ricevere messaggi.

Mamma mia!

E menomale che è un gioco. Non so come operano in FIGB. Nonostante tutte queste precauzioni, non facciamoci illusioni, l'intero sistema rimane veramente vulnerabile, e in passato qualcuno ne ha approfittato.

In questo contesto, lo SquareDeal di Stavaren ci appare sempre più un palliativo per non dire uno *specchietto per le allodole*.



WBF primo utilizzatore

Il nuovo programma, come afferma Maurizio di Sacco in stretto contatto con Stavaren, sarà utilizzato dalla WBF già dalla World Bridge Series (nella **Rosenblum**), con inizio 21 settembre 2018. (vedi allegato).

WBF vuole che il nuovo generatore SquareDeal diventi uno standard per gli organizzatori di tutto il mondo. Bene, questa manifestazione di massima trasparenza da parte della WBF sinceramente mi stupisce visto come si è mossa durante lo scandalo "cheating".

Non capisco come mai il protocollo per gli operatori BBO e relativo software in uso dal 2007 in EBL e WBF non viene passato ed usato in FIGB. In questo caso la standardizzazione a livello mondiale non è applicabile?

FIGB dovrà valutare lo SquareDeal e, se ritenuto idoneo, utilizzarlo per tutti i campionati italiani. Quello che invece chiedo alla FIGB è di pubblicare, nel sito federale, il file (.dup) delle smazzate dei campionati, cosa che attualmente non fa e non si capisce per quale motivo. Da inizio 2018 ciò avviene per i simultanei.

Spettacularizzazione: Sì o No?

Dopo le varie argomentazioni su descritte, due ovvie considerazioni:

1. E vabbeh, ma chi se ne frega se il file delle mani, opportunamente condizionato dall'organizzatore, contiene più manche e slam, **alla fine tutti giocano le stesse mani!** I bridgisti vogliono smazzate

interessanti, e pure gli angolisti di BBO. Possiamo avere un buon centravanti ma se non gli arrivano palloni!

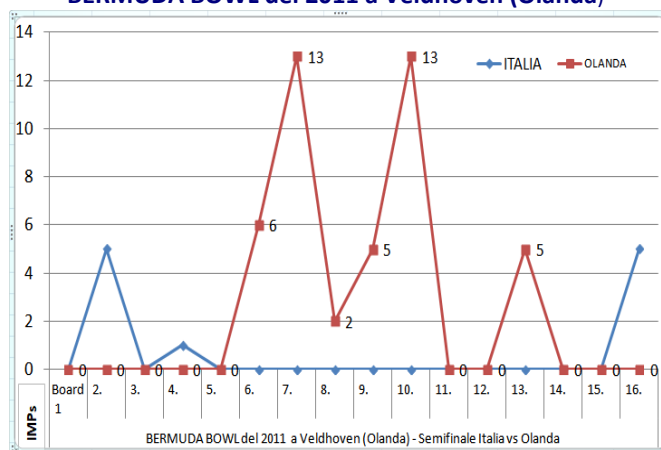
2. Davvero dobbiamo vincolarci allo SquareDeal o ci conviene lasciare carta bianca ai manipolatori seriali? Forse in futuro conviene addirittura legalizzare questo comportamento e così nessuno avrà più nulla da ridire.
3. Volendo possiamo pure organizzare Tornei Tecnici a mani preparate - livello di difficoltà sopra media - e questo anche nei Mitchell locali. Al termine commento finale (nel 2004 in OlonaBridge era già pronta una richiesta alla FIGB in tal senso). Si può provare, come tentativo per richiamare i bravi giocatori ai tornei. Controindicazioni: i falsi prima picche.

Impatto "spettacularizzazione"

Qualche controindicazione sulla "spettacularizzazione" delle mani, in effetti, c'è.

1. In un incontro a squadre, gli slam spostano molti IMP.
2. Un paio di slam in più potrebbe ribaltare la situazione negli ultimi segmenti di gara (vedi grafico sotto).
3. Non è necessario avere in tasca il diagramma delle mani. Gli slam favoriscono la soffiata, magari dell'ultimo minuto, esempio: "alla 4 e 12 si gioca slam" (qualche caso dubbio in passato si è avuto, spesso quando gioca lo sponsor, scarso ma ricco, vince).
4. Più slam ci sono più si agevolano le coppie affiatate dotate di sistemi licitativi più evoluti. Vinca il migliore, sì, però nello stesso tempo si toglie qualche chance ai meno esperti (in un duplicato con 10 mani "piatte" anche le schiappe possono pareggiare contro i big).

BERMUDA BOWL del 2011 a Veldhoven (Olanda)



Ricordo un caso sospetto, almeno a mio parere. Siamo nel 2011, semifinale **Italia vs Olanda** trasmesso da BBO.

Prima del sesto e ultimo segmento, l'Olanda conduceva 157 a 153 IMPs, due slam (board 7 e 10) dichiarati solo dagli olandesi (+ 26 IMPs) eliminarono il nostro Blue Team. Probabilmente all'Italia di **Tamburi & Lavazza** non si voleva dare la possibilità di vincere questa Bermuda Bowl.

E dopo tutto sto' discorso... **NON CI RESTA CHE PIANGERE**

Per chi non l'avesse capito, è evidente che i nostri organizzatori stanno praticando un percorso del tutto irrazionale e, a mio avviso, non più percorribile: mani computerizzate, manipolazioni, diagrammi che girano ore se non giorni prima, soffiare, sala duplicazione isolate, piombate e senza cellulari e Wi-Fi, protocolli, chiavette criptate, enti di controllo, hackeraggio, personale, costi, sponsor agevolati, polemiche, ecc..

Scusate, ma vi rendete conto dove siamo approdati?

Tutto 'sto casino per le mani computerizzate. Forse servirà a qualcuno, ma io sono dell'idea che si può benissimo aggirare l'ostacolo.

A me pare più un gioco di **Guardie e Ladri** che qualcuno si ostina a chiamarlo Sport, forse è per questo motivo che ci viene richiesto il Certificato medico, e qui devo dare ragione al CONI.

Ha senso mantenere un apparato che fa acqua da tutte le parti? Questo gioco, così com'è ora, è uno scherzo che serve solo all'establishment e di certo non porta alcun beneficio alle ASD.

Trasparenza assoluta

Realmente si vuole operare verso un bridge il più trasparente possibile?

Ebbene, per i campionati con mani duplicate, propongo la seguente procedura:

- Trenta minuti prima della gara, in una sala nella sede di gara, alla presenza di giocatori e curiosi, "X" smazzatrici gestite da giovani operatori possono preparare i boards necessari (mani smazzate manualmente dai presenti o dal BigDeal). I tempi ci sono, anzi, avanzano.
- Si preparano due soli boards, tanto per dare inizio alla gara e mentre i giocatori giocano la prima mano = 9 minuti, sapete quanti boards si possono preparare?
- Facciamo un po' i conti. I venditori delle macchinette dicono 600 boards/ora. Ed è vero, l'ho verificato personalmente, comunque sia lasciamo stare i numeri da record di velocità e tagliamo corto: ipotizziamo 120 boards/ora, numeri che anche un novantenne riesce a riempire (le macchinette in questi anni sono divenute sempre più affidabili – si opera con carte nuove). In questi nove minuti si possono preparare tutti i boards sufficienti ad alimentare più gironi di un campionato. Vediamo:
 - 2 x 4 macchinette x 9 = 72 boards.
 - 2 x 3 macchinette x 9 = 54 boards.
 - 2 x 2 macchinette x 9 = 36 boards.

Anche nel calcio mondiale, per evitare le scandalose manipolazioni del passato si sta passando al "VAR".

Tranquilli, questa FIGB - succursale e grande finanziatrice della WBF - non farà alcun tentativo. Figuriamoci! Del resto, il nuovo esecutivo da quando in carica ha rinnovato poco o nulla, in tutti i campi.

Non dimentichiamoci del vantaggio iniziale di 18 minuti. Per gli operatori nessun problema: in 5 minuti di training un qualsiasi ragazzino/a è in grado di operare con le macchinette, diversi circoli già lo fanno senza alcuna difficoltà.

Così facendo si opera con la massima trasparenza, in regime di assoluta sicurezza e si dimezzano pure i costi. Quando vedo le cifre stanziare dal Consiglio Federale per organizzare i campionati a Salso mi vien da piangere.

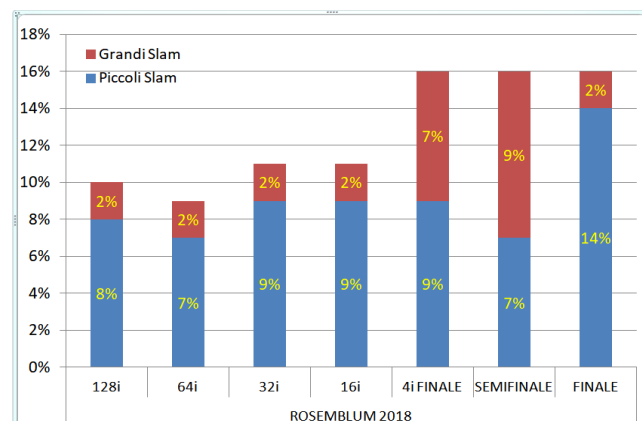
In alternativa, rimango sempre più favorevole al passaggio a un bridge digitale, almeno per le competizioni di alto livello. Il CAS al massimo potrà dire che l'inclinazione dell'iPad non è stimabile.

**Per un
bridge meno
taroccato...**



ROSENBLUM 2018

La WBF, per la recentissima **Rosenblum Cup** (World Bridge Series - ottobre 2018) ha utilizzato il nuovo programma SquareDeal (almeno così afferma).



Come potete notare le fasi finali presentano più slam rispetto alle fasi di qualificazione. Questo anomalo andamento è stato riscontrato anche in altre competizioni. Occasionale? Mah!

Premetto che il mio metodo consiste nel verificare gli slam (potenziali) presenti nel file. Ho analizzato le mani di molte competizioni internazionali, simultanei GP inclusi, e appurato che gli slam prodotti dal BigDeal viaggiano mediamente intorno al 12-13%. Seguirà un articolo in merito.

Allegati/:

1. The Championship Secret - World Bridge Series 2018
2. Il protocollo di gestione delle mani della WBF (traduttore Google)
3. SquareDeal: Tournament Hand Management Software (Hans van Staveren)

The Championship Secret – World Bridge Series 2018

The WBF's dealing hands protocol

Following a proposal jointly put to the Management Committee by Maurizio Di Sacco and Hans van Staveren, in June 2018 the WBF decided to adopt a new protocol for producing computer dealt hands to be used at WBF events.

The original purpose is to avoid any possible suspicion about any kind of manipulation of the hands.

The ultimate goal is to set a standard for all organisers worldwide.

- At a defined moment ahead of a Championship the person responsible for generating and storing the hands – in WBF events Maurizio Di Sacco – randomly generates hexadecimal string of numbers which will be part of the one eventually used to produce the championship's hands (for the World Series 2018 this was done on Monday September 10th).
- That number, called “*the championship's secret*”, will be encrypted in such a way to be impossible to crack.
- The encrypted string will be officially published for everyone to know and store it.
- At the end of the championship the original string will be made public.
- At that point anybody can verify it is the original string: by applying the “ash” method to match the encrypted original code to the published one.
- However, somebody could still claim that the organisation tried a few strings and eventually selected the ones which better suited its purposes (eg using the one which produced wild sets of boards in the crucial rounds)
- To prevent that objection we must add to the string some part that is random, public, and that the organisation cannot control.
- At the moment the protocol claims for the Dow Jones index to be used: upon publishing the encrypted version of the championship's secret we will also publish the date and the time of the day for the Dow Jones index to be used (for the 2018 World Series it will be the DJI at the end of September 14th).
- After that date the whole string will be used to generate all the championship's hands (for the 2018 World Series this will be done any time from September 15th onward).
- Since the format of some events is not yet known (the number of entries is not final) the organisation produced the codes for the Rosenblum Cup, the Open Pairs, the Mixed Teams and the Mixed Pairs. The code for the other events will be generated once the format will be known.
- Here are the original text documents generated by the program. They include all the necessary information:

TN = Tournament Name

KH = Championship's Secret Code

DI = Delayed Information (Dow Jones Index on September 14)

SN = Session: on the right there are the information about how many rounds, how many boards per session, how they are numbered in each of the phases and the hands' file name.

e.g for the Rosenblum, the first SN line reads: 10 rounds; boards numbered cyclically 1-10, 11-20, 21-30; files named ROSQUAL (the ## means that the extension will have a two digit number, here from 01 to 10); event Rosenblum Qualification made out of 10 rounds.

Rosenblum:

TN Rosenblum 2018

KH 25e8f6fcb41f5b16a8fe8944f0d1f693345dac033d214abf0782daa5a87171b5

DI DJI 14/9/2018

SN 10:1-10,11-20,21-30:ROSQUAL##:Rosenblum Qualification #/10

SN 4:1-14,15-28:ROSR64#:Rosenblum Round of 64 #/4

SN 4:1-14,15-28:ROSR32#:Rosenblum Round of 32 #/4

SN 4:1-14,15-28:ROSR16#:Rosenblum Round of 16 #/4

SN 4:1-14,15-28:ROSQF#:Rosenblum Quarter Finals #/4

SN 4:1-14,15-28:ROSSF#:Rosenblum Semi Finals #/4

SN 6:1-16,17-32:ROSFN#:Rosenblum Final #/6

Open Pairs:

TN Open Pairs

KH 7dd8f931aaf36c4155235801fe472a36b752500d5b20ca1280eb415440407fe

DI DJI 14/09/2018

SN 9:1-16,17-32:OPPAIRSQUAL#:Open Pairs Qualification #/9

SN 6:1-16,17-32:OPPAIRSSF#:Open Pairs Semi Finals #/6

SN 2:1-16,17-32:OPPAIRSFIN1_2#:Open Pairs Final Sessions 1 and 2 #/2

SN 1:1-22:OPPAIRSFIN3#:Open Pairs Final Session 3 #/1

SN 3:1-16,17-32:OPPAIRSFIN4_6#:Open Pairs Final Sessions 4 to 6 #/3

Mixed Teams:

TN Mixed Teams

KH 8b277324067d03cda6b5c4cb78a3605107252e04779b554ffa56be87a5bd1231

DI DJI 14/09/2018

SN 10:1-10,11-20,21-30:MXTQUAL##:Mixed Teams Qualification #/10

SN 2:1-14,15-28:MXTR64#:Mixed Teams Round of 64 #/2

SN 2:1-14,15-28:MXTR32#:Mixed Teams Round of 32 #/2

SN 2:1-14,15-28:MXTR16#:Mixed Teams Round of 16 #/2

SN 2:1-14,15-28:MXTQF#:Mixed Teams Quarte Finals #/2

SN 4:1-14,15-28:MXTSF#:Mixed Teams Semi Finals #/4

SN 4:1-14,15-28:MXTFIN#:Mixed Teams Final #/4

Mixed Pairs:

TN Mixed Pairs

KH d6e1971b336e7ac586db84d1747040614cd5fab8cb09f025fd0807647570e13f

DI DJI 14/09/2018

SN 6:1-16,17-32:MXPQUAL#:Mixed Pairs Qualification #/6

SN 3:1-16,17-32:MXPSF#:Mixed Pairs Semi Finals #/3

SN 3:1-16,17-32,1-18:MXPFIN#:Mixed Pairs Final #/3

McConnell and Rand Cup – 2nd qualification day

TN McConnell & Rand 2nd Qualification day

KH 4b4d87761e7a302199ed76df9af3ca04114ff2aec0d0762ce131c7c99a56612f

DI DJI 17/09/2018

SN 5:1-10,11-20,21-30:WSTQUAL2#:Women and Seniors Teams 2nd Qualification day #/5

To be able to verify that the hands were not manipulated in any manner, you should now:

- Copy the Championship's secret for the event you are interested in
- Get a copy of squaredeal.exe at <http://www.xs4all.nl/~sater/SquareDeal.zip> (it includes documentation and instructions).
- Get familiar with the “ash” procedure
- At the end of the championship(s) look for the original hexadecimal string (to be published on the Championship's Daily Bulletin and on the WBF website) and use it to generate the hands: they will correspond to the ones used in the event (in our case, Orlando World Series 2018)

The Championship Secret - World Bridge Series 2018

Il protocollo di gestione delle mani della WBF (traduttore Google)

A seguito di una proposta presentata congiuntamente al comitato direttivo da Maurizio Di Sacco e Hans van Staveren, nel giugno 2018 la WBF ha deciso di adottare un nuovo protocollo per la produzione di mani computerizzate da utilizzare negli eventi della WBF.

Lo scopo originale è quello di evitare ogni possibile sospetto su qualsiasi tipo di manipolazione delle mani.

L'obiettivo finale è quello di stabilire uno standard per tutti gli organizzatori di tutto il mondo.

- In un momento definito prima di un campionato, la persona responsabile della generazione e della memorizzazione delle mani, Maurizio Di Sacco, genera in modo casuale una stringa esadecimale di numeri che farà parte di quella utilizzata per la produzione delle mani del campionato (per le World Series 2018 questo è stato fatto lunedì 10 settembre).
- Quel numero, chiamato "*il segreto del campionato*", sarà crittografato in modo tale da essere impossibile da decifrare.
- La stringa crittografata sarà ufficialmente pubblicata per essere conosciuta e memorizzata da tutti.
- Alla fine del campionato la corda originale sarà resa pubblica.
- A quel punto chiunque può verificare che sia la stringa originale: applicando il metodo "ash" per abbinare il codice originale crittografato a quello pubblicato.
- Tuttavia, qualcuno potrebbe ancora affermare che l'organizzazione ha provato alcune stringhe e alla fine ha scelto quelle che meglio si adattavano ai suoi scopi (ad esempio, usando quello che produceva serie selvagge di tavole nei round cruciali)
- Per evitare tale obiezione, dobbiamo aggiungere alla stringa una parte che è casuale, pubblica e che l'organizzazione non può controllare.
- Al momento il protocollo rivendica l'utilizzo dell'indice Dow Jones: pubblicando la versione criptata del segreto del campionato pubblicheremo anche la data e l'ora del giorno per l'indice Dow Jones da utilizzare (per le World Series 2018 sarà il DJI alla fine del 14 settembre).
- Dopo quella data l'intera stringa verrà utilizzata per generare tutte le mani del campionato (per le World Series del 2018 questa sarà effettuata in qualsiasi momento dal 15 settembre in poi).
- Poiché il formato di alcuni eventi non è ancora noto (il numero di voci non è definitivo) l'organizzazione ha prodotto i codici per la Coppa Rosenblum, le coppie aperte, le squadre miste e le coppie miste. Il codice per gli altri eventi verrà generato una volta che il formato sarà noto.
- Ecco i documenti di testo originali generati dal programma. Includono tutte le informazioni necessarie:

TN = Nome del torneo

KH = Codice segreto del campionato

DI = Informazioni ritardate (Dow Jones Index il 14 settembre)

SN = Sessione: sulla destra ci sono le informazioni su quanti round, quante schede per sessione, come sono numerate in ciascuna delle le fasi e il nome del file delle mani.

ad esempio per il Rosenblum, la prima riga SN recita: 10 round; schede numerate ciclicamente 1-10, 11-20, 21-30; file chiamati ROSQUAL (il ## significa che l'estensione avrà un numero di due cifre, qui da 01 a 10); evento Rosenblum Qualificazione su 10 round.

Rosenblum:

TN Rosenblum 2018

KH 25e8f6fcb41f5b16a8fe8944f0d1f693345dac033d214abf0782daa5a87171b5

DI DJI 14/9/2018

SN 10: 1-10,11-20,21-30: ROSQUAL ##: Rosenblum Qualifica # / 10

SN 4: 1-14,15-28: ROSR64 #: Rosenblum Round of 64 # / 4

SN 4: 1-14,15-28: ROSR32 #: Rosenblum Round of 32 # / 4

SN 4: 1-14,15-28: ROSR16 #: Rosenblum Round of 16 # / 4

SN 4: 1-14,15-28: ROSQF #: Rosenblum Quarter Finals # / 4

SN 4: 1-14,15-28: ROSSF #: Rosenblum Semi Finals # / 4

SN 6: 1-16,17-32: ROSFIN #: Rosenblum Final # / 6

Coppie aperte:

TN Open Pairs

KH 7dd8f931aaf36c4155235801fe472a36b752500d5b20ca1280eb415440407fe

DI DJI 14/09/2018

SN 9: 1-16,17-32: OPPAIRSQUAL #: Open Pairs Qualificazione # / 9

SN 6: 1-16,17-32: OPPAIRSSF #: Open Pairs Semi Finals # / 6

SN 2: 1-16,17-32: OPPAIRSF1N1_2 #: Open Pairs Final Sessions 1 e 2 # / 2

SN 1: 1-22: OPPAIRSF1N3 #: Open Pairs Final Session 3 # / 1

SN 3: 1- 16,17-32: OPPAIRSF1N4_6 #: Open Pairs Final Sessions da 4 a 6 # / 3

Squadre miste:

Squadre miste TN

KH 8b277324067d03cda6b5c4cb78a3605107252e04779b554ffa56be87a5bd1231

DI DJI 14/09/2018

SN 10: 1-10,11-20,21-30: MXTQUAL ##: Qualificazione squadre miste # / 10

SN 2: 1-14,15-28: MXTR64 #: Squadre miste Round di 64 # / 2

SN 2: 1-14,15-28: MXTR32 #: Squadre miste Round di 32 # / 2

SN 2: 1-14,15-28: MXTR16 #: Squadre miste Round di 16 # / 2

SN 2: 1-14,15-28: MXTQF #: squadre miste Quarte Finals # / 2

SN 4: 1-14,15-28: MXTSF #: squadre miste Semifinali # / 4

SN 4: 1- 14,15-28: MXTFIN #: Mixed Teams Final # / 4

Coppie miste:

TN Coppie miste

KH d6e1971b3336e7ac586db84d1747040614cd5fab8cb09f025fd0807647570e13f

DI DJI 14/09/2018

SN 6: 1-16,17-32: MXPQUAL #: Qualifica coppie miste # / 6

SN 3: 1-16,17-32: MXPSF #: Coppie miste Semifinali # / 3

SN 3: 1-16,17-32,1-18: MXPF1N #: Mixed Pairs Final # / 3

McConnell e Rand Cup - 2 ° giornata di qualifica

TN McConnell & Rand 2a giornata di qualificazione

KH 4b4d87761e7a302199ed76df9af3ca04114ff2aec0d0762ce131c7c99a56612f

DI DJI 17/09/2018

SN 5: 1-10,11-20,21-30: WSTQUAL2 #: Squadre donne e anziani 2 ° Giorno di qualificazione # / 5

Per essere in grado di verificare che le mani non siano state manipolate in alcun modo, ora dovresti:

- Copia il segreto del campionato per l'evento a cui sei interessato
- Ottenere una copia di squaredeal.exe a <http://www.xs4all.nl/~sater/SquareDeal.zip> (include documentazione e istruzioni).
- Prendi familiarità con la procedura "cenere"
- Alla fine del campionato, cerca la stringa esadecimale originale (da pubblicare sul Bollettino del Campionato e sul sito web WBF) e usala per generare le mani: corrisponderanno a quelle usate nell'evento (in il nostro caso, Orlando World Series 2018)

SquareDeal: Tournament Hand Management Software

Summary

SquareDeal is a piece of software for people that make sets of bridge hands for tournaments. It uses the well-known program BigDeal for actual dealing, but adds two things:

1. An easy way to make multiple sets of deals for various sessions using consistent naming
2. A way for participants to check the hands were dealt honestly and without any tricks by the organizer

Using SquareDeal a specific procedure is needed, with various phases, by organizer and participants. There is no actual need for participants to do anything, but if they want to check the hands after the tournament they need to do something even before the tournament.

I will describe the phases and in each phase I describe some parts of the software and/or procedures relevant at that phase. The phases follow each other in time, so will describe them after the heading T0, T1, etc.

This document will be released without the software first. The software is running, but needs some work to make it look good. The software is written in Perl(about 300 lines), and will be released both as source and as a precompiled Windows binary. It uses a modified bigdealx, currently called 1.3(BETA). My hope is that after some more modifications having to do with output file formats I will be able to release it as 2.0, but in any case the dealing part is the same as the old 1.2 version. No player should be able to figure out from the hands alone that this set of software is used.

For the random session keys in this document I use a secure random function¹.

At time T0

The tournament organizer(from this point on abbreviated to TO) starts thinking about the tournament and begins preparation. I envision this to be at least three weeks in advance of the first session of play, but maybe even earlier.

He starts up SquareDeal and tells it a new tournament is coming. He needs to supply a short name, to be used as filename prefix. Let us be original in this document and call it *test*. The program will now make two files, *test.sqd*, which contains the description of the tournament and will be published before the tournament and *test.sqk* which will contain the keys and will be published after the tournament.

There will be four options:

1. Set Tournament Name
2. Set Delayed Information Description
3. Add phase of tournament

4. Publish

The tournament name is just a string for description, and will not be used for any operational purpose. Something like “Bermuda Bowl 2023 Oct 2, Vatican City”.

The delayed information description describes which specific information will be used as delayed information. More about this later. Something like “DJI index September 29”.

Each tournament is expected to have various phases, like Round Robin, Quarter Final, etc. Each phase will have multiple sessions.

The information for each phase contains the following:

1. The number of sessions
2. The number of boards per session. This can either be a simple number, like 16, or a range, like 17-32. It can also be a list of things, like 1-16,17-32. In the latter case the program will cycle through this list, in this case 1-16 and then 17-32 and then 1-16 again.
3. The file prefix. This is identical to the normal one for BigDeal with one exception: any string of # characters will be replaced by at least the same number of digits for the session. So suppose the prefix given is brrr## and we generate session 7, the file prefix will be brrr07.
4. The description. A string, non-interpreted, that will be displayed when making the hands. Same trick with the # characters. Example: “Bermuda Bowl Round Robin #/23”

Apart from writing all this info in the description file the software will generate a (very) big random number for each sessionⁱⁱ, and stores it in the .sqk file.

The TO can enter and exit the program various times, and continue where he left off.

At time T1

At a certain point the TO is finished with preparing the tournament. He chooses the publish option(#4) which terminates the first phase of the program. Now he receives a message telling him to publish the .sqd file and keep .sqk file very very secret.

Publishing the file can be done in various ways. I envision putting it on the tournament website and/or Emailing it to all participants. We will see how this turns out.

Keeping the key file very very secret would require at the least an encrypted USB stick or similar measure. Keep in mind that if the contents of this file would leak before the end of the tournament players will be able to generate the hands themselves before the session.

At this point interested players can do something. They can make a copy of the .sqd file as published. There is not a lot they can do with the file now, but the file contains a signature of all session keys, and they need that after the tournament to check. If they do not make a copy a devious TO could change the keys and repost the .sqd file with a new signature.

Time T1 could be the same day as T0, or much later, but it should be some two weeks before T2.

At time T2

This is the point where the Delayed Information comes to life. What is the Delayed Information(DI) and why is it needed? The DI is any info, chosen by the TO, but such that everyone will be able to figure out that the TO could not have known it at time T1. A DJI index, the gold price, the drawing of the Italian state lottery, anything is OK, including combinations of things. The only rules:

1. The TO cannot have known the info at time T1. Preferably nobody should have been able to know it then.
2. At tournament time anybody should be able to know this information. Preferably it should stay known forever, for everyone to see.

Why do we need it? If the hands for the sessions would only depend on the session keys the TO could plan them in advance. As we will see later the DI modifies the session keys in a major way. As long as the info in the DI contains a reasonable number of bits(20 or so) it becomes difficult for the TO to change statistical properties of hands. Even very suspicious players would be satisfied with 40 bits. Picking 6 from 49, say a Lotto type game produces about 24. Combine that with the DJI and you are in a very safe zone.

Anyhow, at time T2 the TO calls the program again and sets the now known DI. The players can look up the number if they wish, but can also do that later.

At time T3

Tournament time is almost there. The duplication room is being set up and the TO needs to generate hands. Call the program and use the generate hands option. You can specify a phase, and within the phase one or more sessions. Session numbers can be a single number(make one session), a list like 1-10(make the first 10 sessions), or a * meaning all sessions.

The TO has no choice now, the hands will follow straight from two(three) pieces of information, the session key, the DI(and a reserve set number). This normally finishes what you can do. There is however one emergency option: if as a TO you screw up, or someone from your staff does it could be that in hopefully rare circumstances the hands for a session leak out(it has happened that hand records from session 4 were distributed after session 3). So there has to be a way to make reserve hands. This option exists, you can even make an infinite amount of reserve sets.

Having made reserve sets however the TO is obliged to tell the players this. This can be done now and/or at time T4. A TO that needs to do this more than once per 5 tournaments is either very sloppy, or he is still rigging hands.

A reserve set is made using the session key, the DI and the reserve-number.

At time T4

The tournament is finished. The TO now publishes both the updated .sqd file and the .sqk file. He also states if he has used reserve sets and which. Here his responsibility stops.

Interested players can now download these files and run the software themselves. The software will check the signature of the keys(or they can use standard SHA-256 software) and the players can now

make all the hands of the tournament, comparing them to what they actually played. Any mishap here requires investigation and detailed explanation by the TO.

Hopefully it will never come to that, and furthermore before starting to accuse TO's it would be a good idea to check the software. Contact me at sater@xs4all.nl, maybe I screwed up.

Connection to BigDeal

This software uses the bigdealx version of BigDeal. Normally the ReadMe states that you should not. Given that I claim I know what I am doing I still use it.

There are three modifications:

1. BigDeal used a 160 bit hash of an owner string as extra entropy. Because now the TO and the suspicious player have to use exactly the same starting value I cannot use this owner string.
2. Normally using dangerous flags to BigDealx causes it to scream and convince you not to do it. We changed it not to scream when using the right flags.
3. Normally BigDeal in the x version complains very loudly of regenerating sets of hands. With this software regenerating sets of hands can happen easily if you just lost your session 3 of phase 2. Now we do not.

Implementing these three changes was done by adding a -W option (Wizard...) with a string as argument. This string is the first half of the session key (about 175 bits for a 160 bit hash). The other half of the session key, and the DI and the reserve numbers are added with -e switches.

So, pointing you to the BigDeal online info, the hands in BigDealx with -W string are now generated by running the following three things through a RIPEMD-160 hash:

1. The 160 bit hash of the first half of the session key
2. The 160 bit hash of the second half, plus the rest
3. An increasing counter

After that all other normal BigDeal things happen.

File formats

The formats of the .sq? files are:

Test.sqd

```
TN Test Tournament
KH 2a138794640b2f3580390e1b5866277fd074f29069c4e2c80751e4c94c03cee3
DI DJI April 13
SN 23:1-16,17-32:testrr##:Round Robin # of 23
SN 7:14:testfin#:Finals # of 7
PU
```


Test.sqk

```
1,1:B1oGWihtYumKlpGatFw6Axv4v7TBBBINKsWhVFzpzAAvea3qfvhZddkg00tL
1,2:ypY9fWFCzqaD1LiCEK6Xg03znnv6lMf1e9exXykYt1bnppc4B4oKGmzaSVxU
1,3:U2USDtPp3DH3xX1Ea3y1UhHauYLuygFl0j58EZUiQPbMy71IudKKjupcizpk
1,4:XowkYV4E0n1WHqIdKvveekduCGjEocAIOTMkb7fB1GdYVWYDR8FNO9czOxmE
1,5:IwSnFLD45Rq7plDVQHYHpOn88EWS2RgeqgMH8ZeBcIJ36GrfqLLDdgXWFrMm
1,6:nSHSiZbrFJyGA6NCKBTyrsXwj dGJzF3lxWK4pdCfael6UQz4QrSnN7NZZGMB
1,7:wqKrPVsN1aXrb1ZjOUCEBafP2xvOUsidPh8ennV6wh9MmTHNyfEJ5YorASW
1,8:b77BJNly34jrxikYqXALIEOmoK5mck27ugcv1rg5j8qqtn9JKHoRDwsj2HkF
1,9:tJ12G7NodX33R0i12DcVxjft115rrG1hQQuHtIBsvZ6pyvBw5Nbrd7tNephK
1,10:JGKagH9CAmVlSPqfd3vAoPNTVm2L4l3FaTQRHwjf7RGH0XfTf9Ath85LhTc5
1,11:USvmUOaXChBiViYOQkPTV6VwHLT4jIxhdO6vALMWUjCPWYaWX2iZfRuYqF2o
1,12:dv9L9aYfL9HEa9r99fxTCJTAevlkbQufna34ZpGgptkISC2Nc2WzcihLX8Qi
1,13:NZnvPV7D1rbnaEXew52mqqYOAbz9tVRrihnexaGe4vORhW3z45fvrOcwyrN
1,14:1RoVxXTYog7gllaFsFKe74szI1SIFKNZ0WbEnjbI5sKcBvL3OcZaUXs20GuK
1,15:GIjsWBJR2ti04dQ6ZUsYpWbEuRQv4gDih5Qw9f2psvqLPt4gJLVQTNyOCd7H
1,16:KJ4nNjboFutOWdYDgcFscERu4Rky0xRx8BWM0SylNlJG0NqdYAtWC7JILuIw
1,17:Oa5na6xnetUKdURLpAAZefWQc3halZHLgGIVjdk7ZkhshIAagbzYKRdYAYUi
1,18:5ObZvlRRm27EnseP2KsMu5R3QtIHG8PnQbmRQuOkxE8XDSvajgeUJD8x6Qxj
1,19:cfSIUG2EdpqrBaeSPCC6rEGV4WXHL1FCgSN3xiWdQZanaaeNC6xg40gyFilB
1,20:e7T7FFu0eKcpGAiLfHKHogJaT2WJUqSULyJgxvJZa5ugXTATeUGZb77m3V9I
1,21:CNVfA6TMypBxeFT5D3K1sHUMRddlvoUis6quAse28F5ctTTd6FUW3BkayHof
1,22:KFdz3l0eeZGsLDHNS2OB0f4cG09xUlXPULPk9He8rEf4Afbx06WJa9K2tI2v
1,23:zKRAG1ZzrAlSClOiPh8oaqKMq9u5q6CVJwKiLDxmnYM5u90tT6xz0HsIXyPq
2,1:WKirJbd9ibhLwd4ueUDtWFSP1oErsKRopM1Erwy387xuKGB0RgmwhOJIZNjv
2,2:Bb65fAaN0mi5JhCKVU2MFjzKev7WEyfnRbTIWsX6WV65E0tCVmbCqwJXpBNn
2,3:BVDqXOEDr6hAuJVLKJ8LsL57uVvQbI7QpPhZ3AcRGgZW100AeQ3hFpkGC3Mq
2,4:AR1Gu2QxOjLTzVttUHXFrWUqvFcYOVkjheNgtke2BdEW5PYcu3EjM4glhUuC
2,5:rNpUiGfmcH7isNOnOSkONEMI2mwCN55jbVgRjHVZciUnd0ty41UacTaIF14k
2,6:F9zF3AugyAbyQYnbfSUwZ3QK7ZgHsa2PYcW3ZZ02wAam2cN6Fr1YWn2THixM
2,7:56BDv9PZ2eQxVu5ZHHysffvsUVKQcKBxHbB7DDyOJbx2avwZaICdK641Wgdb
```

For the keyhash I use the SHA-256 function. The annoying detail you have to figure out is the line termination. On Unix type systems line termination is `\n` or `NL`, while on DOS like systems it is `\r\n` or `CRLF`. Normally you could not care less, but for this keyhash it is important you do it consistent. I chose to use the DOS like convention.

Conclusion

This will say something smart later.

ⁱ perl Bytes::Random::Secure::random_string_from function which is supposed to use the OS secure random generator

ⁱⁱ 60 characters with 62 possibilities equals about 357 bits