Niniejszy dokument opisuje procedurę generowania rozkładów rozdań opracowaną dla WBF przez Hansa van Staverena, a zaadaptowaną przez PZBS w celu poświadczania, że rozkłady rozgrywek są generowane losowo, a osoba odpowiedzialna nie może rozkładami manipulować.

PZBS wdraża obecnie tę procedurę pilotażowo w ligach centralnych, a w dalszej kolejności rozważa się wdrożenie jej w innych najważniejszych rozgrywkach PZBS.

Wprowadzenie

Wykorzystywane nazwy i terminy:

- Organizator - organizator zawodów lub osoba przez niego upoważniona do wygenerowania rozkładów rozdań na zawody.
- BigDeal - generator rozkładów rozdań autorstwa Hansa van Staverena, od kilkunastu lat powszechnie używany przez WBF, EBL, PZBS oraz przez innych organizatorów rozgrywek brydżowych na świecie, wielokrotnie weryfikowany i nigdy nie podważony.
- Ziarno (ang. seed) - liczba podawana programowi BigDeal, na podstawie której generuje on ciąg zestawów rozdań. Ziarno może być liczbą potencjalnie bardzo dużą, do ok. 1,5 x 10^48 (podczas gdy liczba wszystkich możliwych rozdań brydżowych to "zaledwie" ok. 5,4 x 10^28). Wielokrotne podanie tego samego ziarna spowoduje wygenerowanie tego samego ciągu rozkładów. Podanie na starcie innego ziarna (choćby tylko nieznacznie zmienionego) spowoduje wygenerowanie zupełnie innego ciągu rozkładów. W ujęciu matematycznym, generator rozdań jest funkcją odzwierciedlającą ziarno w ciąg rozkładów rozdań.
- Opóźniona informacja - pewna wartość liczbowa, o której wiadomo, że nikt nie może jej znać przed określonym terminem, nikt nie może wpłynąć na ustalenie jej konkretnej wartości, a po upływie tego terminu jest precyzyjnie ustalona i publicznie znana. Przykładem takiej informacji jest wynik określonego losowania Lotto.

Niniejszy dokument nie ma na celu wnikliwego wyjaśnienia zasady działania BigDeala. Zostało to już wyjaśnione naukowo przez samego autora (ang.), sprawdzone przez ekspertów, a także zaprezentowane w formie popularno-naukowej przez Konrada Ciborowskiego w "Brydżu" nr 12/2008 oraz przez Mirosława Męcika w jego wykładzie o generowaniu rozdań z 2005 r.

Niniejszy dokument ma na celu zaprezentowanie procedury, która poświadcza, że organizator nie może manipulować pojedynczymi rozkładami, a także nie może wygenerować wielu zestawów rozdań i dokonać ich selekcji czy zmiany kolejności, a więc, że używane rozkłady powstały w sposób losowy oraz w taki sam sposób zostały przyporządkowane do poszczególnych sesji rozgrywek.

Procedura

1. Pewien czas przed zawodami organizator generuje dużą liczbę (o rozmiarze jak ziarno), tzw. sekret, po czym publikuje sekret w postaci jego tzw. hasha, tj. wartości będącej wynikiem wykonania funkcji skrótu (funkcji hashującej). Sam sekret pozostaje poufny.

2. W tym samym czasie organizator określa i podaje do publicznej wiadomości opóźnioną informację, której wartość jest w tym czasie jeszcze nieznana, ale stanie się publicznie znana jeszcze przed zawodami.
3. Gdy opóźniona informacja jest już znana, organizator generuje rozkłady rozdań, używając połączenia sekretu i opóźnionej informacji jako ziarna dla BigDeala.
4. Po zawodach sekret zostaje opublikowany.

Weryfikacja

Po zawodach każdy może zweryfikować, że rozkłady powstały w sposób losowy, w następujący sposób:

1. Pobrać sekret opublikowany przez organizatora i zweryfikować, czy opublikowany przed zawodami hash był prawidłowy.
2. Pobrać rozszerzoną wersję programu BigDeal i za jego pomocą użyć ziarna (sekret wraz z opóźnioną informacją) do wygenerowania rozkładów. Najprościej przeprowadzić to w następujący sposób:
    a. Organizator publikuje pliki w formacie oczekiwanym przez program: plik *.sqk zawierający sekrety dla poszczególnych sesji rozgrywek oraz plik *.sqd zawierający m.in. hash pliku *.sqk, wartość opóźnionej informacji oraz definicję poszczególnych sesji.
    b. Pliki należy umieścić w katalogu programu i uruchomić squaredeal.exe.
    c. Następnie należy postępować zgodnie z instrukcjami wyświetlanymi na ekranie (ang.) i wybrać opcję “make session(s)” w celu wygenerowania rozkładów.
    d. Przy pierwszym generowaniu trzeba będzie odpowiedzieć na dodatkowe pytania o formaty generowanych plików.
3. Zweryfikować, czy te rozkłady były rzeczywiście wykorzystane podczas zawodów oraz czy w odpowiedniej kolejności.

Proszę zauważyć, że:

- Nikt poza organizatorem nie może odtworzyć rozkładów przed zawodami, ponieważ funkcja skrótu jest nieodwracalna, tzn. z opublikowanego przed zawodami hasha nie da się uzyskać pierwotnej wartości - sekretu, który jest składnikiem ziarna.
- Organizator może spreparować sekret, zamiast wygenerować go losowo, ale nie pozwala mu to na selekcję rozkładów czy manipulowanie poszczególnymi rozkładami, ponieważ nie zna z góry wartości opóźnionej informacji, która stanowi część ziarna. Nawet najmniejsza zmiana ziarna skutkuje zupełnie innym ciągiem rozkładów.
- Organizator nie może użyć i opublikować po zawodach innego sekretu, niż początkowo ustalony, ponieważ znalezienie innej wartości wyjściowej, dla której funkcja skrótu zwróci ten sam hash, jest praktycznie niemożliwe (jest to cecha funkcji skrótu).

Dnia 8 listopada 2018 r.
Opracowali: Michał Zimniewicz, Marcin Wasłowicz