RNGs and Things – Dispelling the Myths and Misconceptions about the Fairness of Online Poker

All In Magazine: April 2007

Sometimes gamblers have more old wives' tales than old wives, and the world of online poker is no exception. Winning strategies abound, but are you basing your strategy on superstition and fairy tales, or mathematical fact.

Whether you're playing poker over the Internet, or dropping quarters into the poker machine at your local watering hole, the same principles apply. It's all about electronic gaming, and it's all about understanding the science behind the action. If you're not applying strategies that make sense, then you could be reducing your chances of winning and increasing your losses.

The first and most common myth about online poker is that the games aren't really random, because you're not using a real deck of cards. On the contrary, as long as the poker room is designed correctly, and subjected to independent testing and verification, the card dealing should be determined by a reliable and trustworthy 'Random Number Generator (RNG)'.

An RNG is an electronic component used for generating game outcomes. There are two basic types of RNGs: software and hardware.

At the heart of every software RNG is a mathematical algorithm. Software RNGs are also known as pseudo-RNGs because these algorithms generate outcomes that only *appear* to be random. Some would argue that the pseudo-random behaviour of software RNGs makes them inferior to hardware RNGs. This is a classic misconception. Just because software RNGs are only pseudo-random, doesn't mean they can't get the job done. When implemented correctly, software RNGs can be sufficiently random for any gaming application. On the flipside, when designed poorly, software RNGs can show a bias or pattern that could potentially allow players to predict the game outcomes.

Hardware RNGs are altogether very different. Hardware RNGs are comprised of a physical hardware device (usually an electronic card that plugs into a computer) complete with special interface software. Hardware RNGs are capable of *truly* random output. Since hardware RNGs do not depend on an algorithm, they are not subject to the limitations of pseudo-random behaviour. However, there are other issues that must be addressed when using hardware RNGs. For example, since hardware RNGs are comprised of physical hardware devices, they can potentially wear out and break down over time.

Some gaming websites even use a combination of both hardware and software RNGs together.

Another classic misconception is that the eventual outcome of the game depends on how fast or how slow you bet, or what amount you bet.

With either type of RNG (software or hardware), as long as it is designed correctly there shouldn't be any way to cheat the game – regardless of when you press the play button, how much you bet, or any other factor that clearly shouldn't impact the game fairness.

In most poker room implementations, the RNG is designed to randomly shuffle the deck and determine the value of any face-down cards during the initial card dealing, just like in a real game. In addition to more accurately simulating a real-life card game, this also allows the poker room to store incomplete games in the event of a power failure or similar system crash, thereby providing a mechanism to complete those games upon re-start.

This of course gives rise to another misconception about online gambling: that the game outcomes are known in advance by the website operators, and therefore can be used by the operators to win their own games.

Again, as long as the RNG is designed correctly, there shouldn't be any way to cheat the game. A properly designed RNG should keep any hidden values secure from all illicit access – be it from an external or internal source.

When it comes down to it, the game outcomes are determined purely by a combination of the RNG-driven card dealing, in conjunction with the players' choices in the game. Since the players can't control the card dealing, they should be left with only their skill at the game of poker. This means understanding the natural probabilities of card outcomes when playing with one or more decks, and observing the patterns of your opponents in order to anticipate their moves.

This in turn relates to yet another misconception about online gambling: that unfair player collusion cannot be stopped, and that you are powerless against rings of conspiring players. On the contrary, as long as the poker room is designed correctly the operator should have controls in place to monitor and detect player collusion. Naturally, no system is perfect, but many collusion rings have been caught and banned from online poker rooms. Complex algorithms are implemented to search for behaviour patterns that are consistent with player collusion. This is augmented by operational procedures put in place to actively monitor players with increased winning percentages. If someone's winning percentage is much higher than normal, then this might be an indication of cheating.

This leads us inevitably to the last, and probably the most dangerous myth about the online gambling industry: that all poker rooms are created equal. After reading all of these facts about RNGs and poker room monitoring, a smart reader is probably thinking, *"Sure, but how can I trust a website operator to implement all of these systems to make sure that the games really are fair and random?"*

That's a very good question. Unfortunately, there's no easy answer.

In order to better understand the situation, one must first understand the regulatory structure of the gaming industry. Each poker room is hosted from a particular gaming jurisdiction. There are a number of gaming jurisdictions around the world, each with a unique set of standards and rules, and a unique approach to licensing and monitoring the websites under their supervision. These regulations can span a wide range of areas, such as operational policies and procedures, financial controls and technical design specifications. Most importantly, different gaming jurisdictions have different approaches to enforcing their regulations.

For example, most highly-regulated gaming jurisdictions enforce strict requirements for RNGs to ensure that the games are fair, random and non-predictable. Accordingly, players that choose to wager on websites hosted from those jurisdictions can enjoy a certain degree of assurance that the game outcomes are fair, and that their wins will be paid out correctly. Jurisdictions such as Alderney, the Isle of Man, Vanuatu and Australia, and even promising, relatively newer jurisdictions such as First Cagayan in the Philippines are widely-recognized as having a strong regulatory framework. This list is by no means exhaustive, but it is instead intended to provide a sample of known highly-regulated gaming jurisdictions.

Conversely, players that choose to wager indiscriminately on websites hosted from unregulated or poorly-regulated gaming jurisdictions are subject to the whim of the website operators, which unfortunately cannot always be relied upon. These operators *could* be honest or dishonest, but without an appropriately and enforced regulatory regime, there's no real way to be certain.

So what can online poker players do to protect themselves from shady operators? Players can take steps to increasingly protect themselves by researching their choices carefully. There are a significant number of fair and honest poker rooms available. Unfortunately, there may also be a number of websites run by dishonest or unscrupulous operators. The best approach is to learn about the different gaming jurisdictions, as well as the different types of regulatory compliance testing that can be applied to a poker room, and subsequently make a decision based on these facts.

Whether you're trying to avoid shady operators, or trying to beat the best players in the world, knowledge is both your best defence and most significant advantage. That's much better than relying on a rabbit's foot or some winning scheme you happen to chance across on the Internet or late night TV.

<u>Bio</u>

Mr. Noah Turner is the Chief Technical Officer (CTO) of Technical Systems Testing (TST), an internationally recognized Accredited Testing Facility (ATF) offering evaluation and consultation services for both the land-based (traditional / terrestrial) and Interactive gaming, lottery and Information Technology (IT) industries.

Office: +1 (604) 873-5833
Email: nturner@tstglobal.com

<u>OFFICES:</u>
Vancouver *– Suite #420, 1367 West Broadway, Vancouver, British Columbia, Canada, V6H 4A7 //* ***O:*** *+1 (604) 873-5833 //* ***F:*** *+1 (604) 873-1075*
London *– Swan Centre, Fishers Lane, Chiswick, London, England, United Kingdom, W4 1RX //* ***O:*** *+44 (0)2087 474 956 //* ***F:*** *+44 (0)2087 427 967*
Sydney *– Suite #305 / 306, 30 – 40 Harcourt Parade, Rosebery, New South Wales, Australia, 2018 //* ***O:*** *+61(2) 9700 7023 //* ***F:*** *+61(2) 9700 7024*
Melbourne *– Level 28, 303 Collins Street, Melbourne, Victoria, Australia, 3000 //* ***O:*** *+61 (3) 9678 9095 //* ***F:*** *+61 (2) 9700 7024*
Macau *– Macau Number 39, 17F Central Plaza, 61 Avenida de Almeida Ribeiro, Macau, China //* ***O:*** *+853 8291 3992 //* ***F:*** *+853 8291 3889*