# Randomised Proofs

Dic Bolony
A University of Yon Queen Length Clods

**Abstract**

The full power of randomness is finally unleashed. A remarkable new proof paradigm is proposed. This could revolutionise the whole field of craptology, and the results will undoubtedly spill over into other disciplines too.

## 1 Introduction

Use of randomisation in cryptography has a long and distinguished history. Cryptologists have long known that good cryptosystems should possess similar properties to random functions and have proposed many *pseudorandom* functions for this reason. True randomness has also been used in homophonic coding and, more recently, in interactive protocols.

Provable security is a relatively recent concern of cryptologists. Randomisation has recently started to appear as a component in proofs for cryptography in various ways. The purpose of this paper is to show that this trend deserves to be extended much further than it has been so far. Only by fully randomising proofs can the idea be brought to complete fruition.

## 2 Previous Work

In recent years there has been a clear trend towards a significant, but limited, exploitation of the true power of randomness in proofs. There have been many papers in which the technique, which we here call *pseudorandom proof*, has been used. This technique works as follows.

1. Write down sequentially each element that is to be used in the proof on a separate sheet of paper.
2. Shuffle the sheets randomly.
3. Write out the proof in the new order.

This proof technique has used to provide an incredible number of startling new results which have been forthcoming in recent years[1]. However, these proofs become completely

[1]Although there are many examples, it would be unfair to attribute this technique to any specific authors since it has seen such a gradual assimilation into the literature.

devoid of randomness once they have been committed to the printed page. What these authors have failed to grasp is that the true power of randomness can only be realised by using *dynamic proofs* which must change *every time they are read*. Now that this revolutionary idea has been discovered it quickly becomes clear how to unleash the power of randomised proofs.

# 3 Truly randomised proofs

How can we introduce true randomisation into a proof? Music and literature provide the clue. Mozart produced a set of minuets in which a set of dice must be cast in order to generate a new tune to be played every time [1]. Stine [2] has shown that literature in which a story is designed dynamically while being read can add an extra dimension. From here it is only a small step to discovering proofs which can be randomised in real time. The general technique works as follows.

1. Write down and label sequentially $2^k$ random assertions concerning the proposition to be proven.

2. Toss a random coin $k$ times.

3. Read only the the assertion labelled by the string found in step 2.

It is clear that the power of this technique stems from the inspirational idea to move randomness from the *writer* of the proof to the *reader* of the proof. The following powerful theorem follows almost immediately.

**Theorem 1** *Randomised proofs are incorrect with negligible probability.*

**Proof** The probability of reading a particular assertion is clearly $1/2^k$. Therefore, even if this assertion should turn out to be false, the chances of reading it are negligible. □

In a series of follow up papers we will show how to use this technique to establish new results, many of which it has previously been thought could never be proven.

# References


[1] Zs. M. Ruttkay, Composing Mozart variations with dice, `http://www.cwi.nl/~zsofi/mozart/`.

[2] R. L. Stine, Give Yourself Goosebumps #6, Beware of the Purple Peanut Butter, Scholastic.