Pseudo-Random Number Generation Using Adversarial Neural Networks

Marcello De Bernardi*, Martin Abadi†, Pasquale Malacaria‡, Arman Khouzani§
*School of Electronig Engineering and Computer Science
Queen Mary University of London, London, United Kingdom E1 4NS
Email: m.e.debernardi@se15.qmul.ac.uk
†Twentieth Century Fox, Springfield, USA
Email: homerthesimpsons.com
‡School of Electronig Engineering and Computer Science
Queen Mary University of London, London, United Kingdom E1 4NS
Email: p.malacaria@qmul.ac.uk
§School of Electronig Engineering and Computer Science
Queen Mary University of London, London, United Kingdom E1 4NS
Email: a.khouzani@qmul.ac.uk

***Abstract*—*Pseudo-random number generators* are a fundamental element of many cryptographic systems such as *encryption algorithms*. As PRNGs are often a single point of failure for such systems, their design and analysis is an important field of investigation. While *deep neural networks* have been tremendously successful in recent years, little effort has gone into their application to the implementation of PRNGs. Some relatively obscure and complicated attempts have been made with little success.**

This investigation pursues a simple and elegant novel approach to the problem, by proposing the use of *generative adversarial networks* to train a neural network to behave as a cryptographically secure PRNG. This is a natural association, as a GAN closely resembles the adversarial nature of security problems. Furthermore, this work showcases a number of interesting modifications to the standard GAN architecture. The most significant is training the GAN's generator network to produce outputs that the adversary network cannot predict, rather than training the generator to mimic as reference distribution as is standard. Thus the pseudo-randomness property in the generator's output is formulated in terms of unpredictability by an improving opponent.

Using the NIST statistical test suite to evaluate the performance of the generator network, this work investigates the extent to which training the proposed models improves their performance as a PRNG, and discusses the possibility of using the models in a cryptographic context.

This report demonstrates that a generative adversarial network can effectively train the generator to produce pseudo-random number sequences with good statistical properties. At best, the trained generator could pass around 99% of test instances and 98% of different tests. These very strong results outperform most other results in the field, and are achieved with a much simpler and robust approach compared to previous attempts. While these metrics alone are not sufficient to justify use of the models in a cryptographic setting, there is a strong case for further investigation and improvements to the design.