Lightweight true random number generators a step closer

September 20 2010

The widespread use of true random number generators (TRNGs) has taken a step closer following the creation of the most lightweight designs to date by researchers at Queen's University Belfast's Institute of Electronics, Communications and Information Technology (ECIT).

Members of the Institute's cryptography research team have produced a series of circuits that are up to 50 per cent smaller than anything else currently available. Optimized for digital circuits, FPGA and ASIC, they push efficiency to the limit by using just one logic gate, one look-up table and four transistors respectively.

TRNGs are essential for IT security because virtually any security application relies on unpredictable numbers such as cryptographic keys. Current systems however are either too expensive or are not fast enough for many applications. That is why more nimble pseudo-random number generators are in widespread use even though the sequences they generate can be detected under certain types of attack, making them much less secure.

The approach of ECIT researchers Jiang Wu and Dr Máire O'Neill has been to use the white noise inside the circuit to generate the randomness, effectively simulating the toss of a coin. To do this, they developed a new mechanism to measure the noise and generate the random output.

"The most challenging part of the work was to find the new mechanism that can effectively sample the noise," said Wu.

"True random number generators have been extensively studied in recent years; many very efficient designs based on different noise measurement mechanisms have been proposed. It was not clear if more efficient designs were even possible. After investigating several candidates, finally we found a successful one."

The next step is to find ways of making the generators sufficiently robust to be embedded in devices such as mobile phones, smartcards and RFID tags, and - where they are used for security applications - to secure them from attack and develop appropriate countermeasures.

Other related work currently underway at ECIT includes designs for highly efficient physical unclonable functions (PUFs). These authenticate individual chips by extracting and identifying - but without revealing - their unique fingerprints which can then be used in a variety of security applications.

Provided by Queen's University Belfast