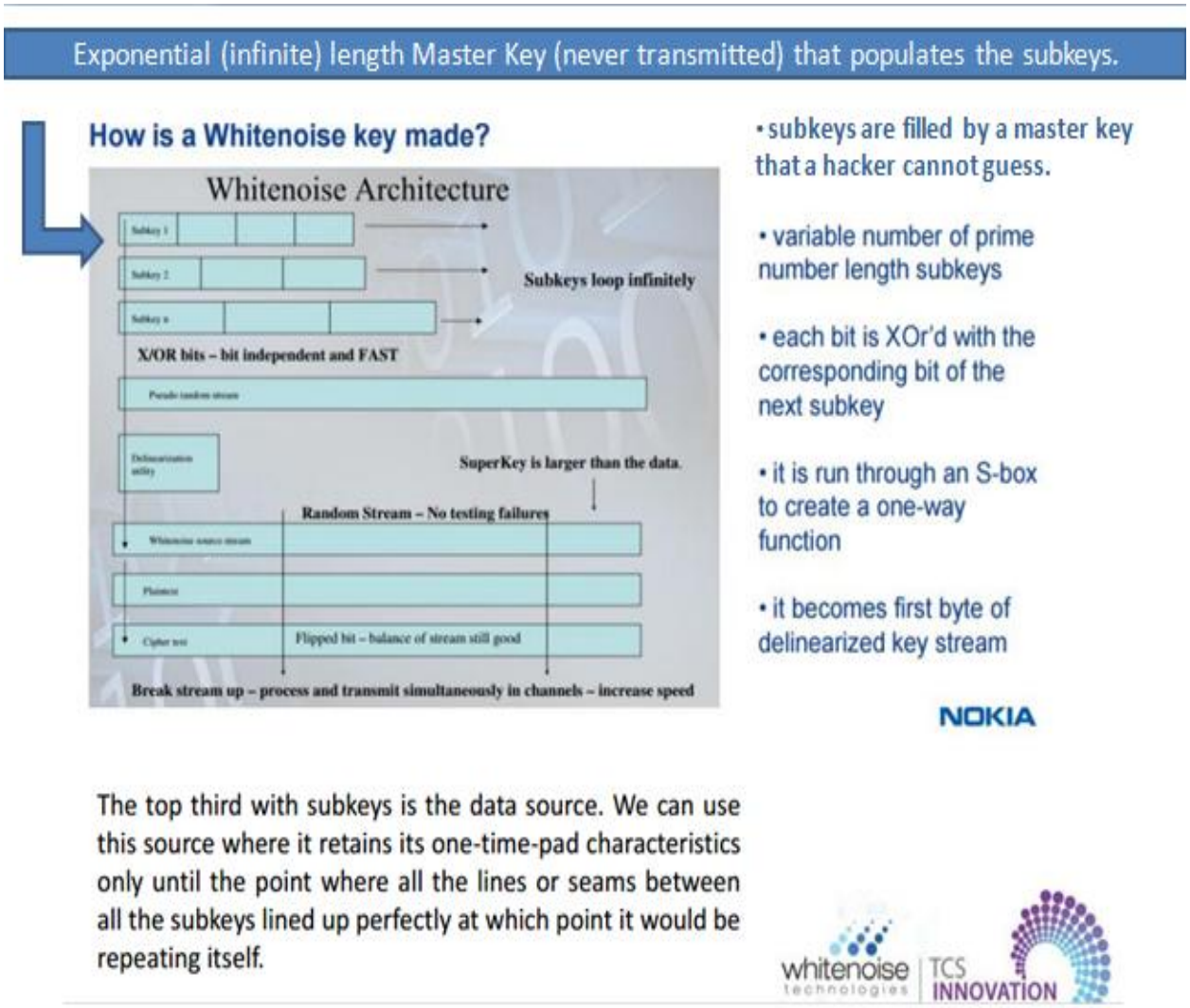
Three reasons why side channel attacks don't work on Whitenoise

In Figure 1 we see how a Whitenoise key is made and the one-way-functions that prevent hacking. A whitenoise key is made up of a variable number of prime number length subkeys. They are like troughs and they are populated with deterministic random data from the Master Key which has never been transmitted or shared. See arrow.

Fig 1



The top third with subkeys is the data source. We can use this source where it retains its one-time-pad characteristics only until the point where all the lines or seams between all the subkeys lined up perfectly at which point it would be repeating itself.

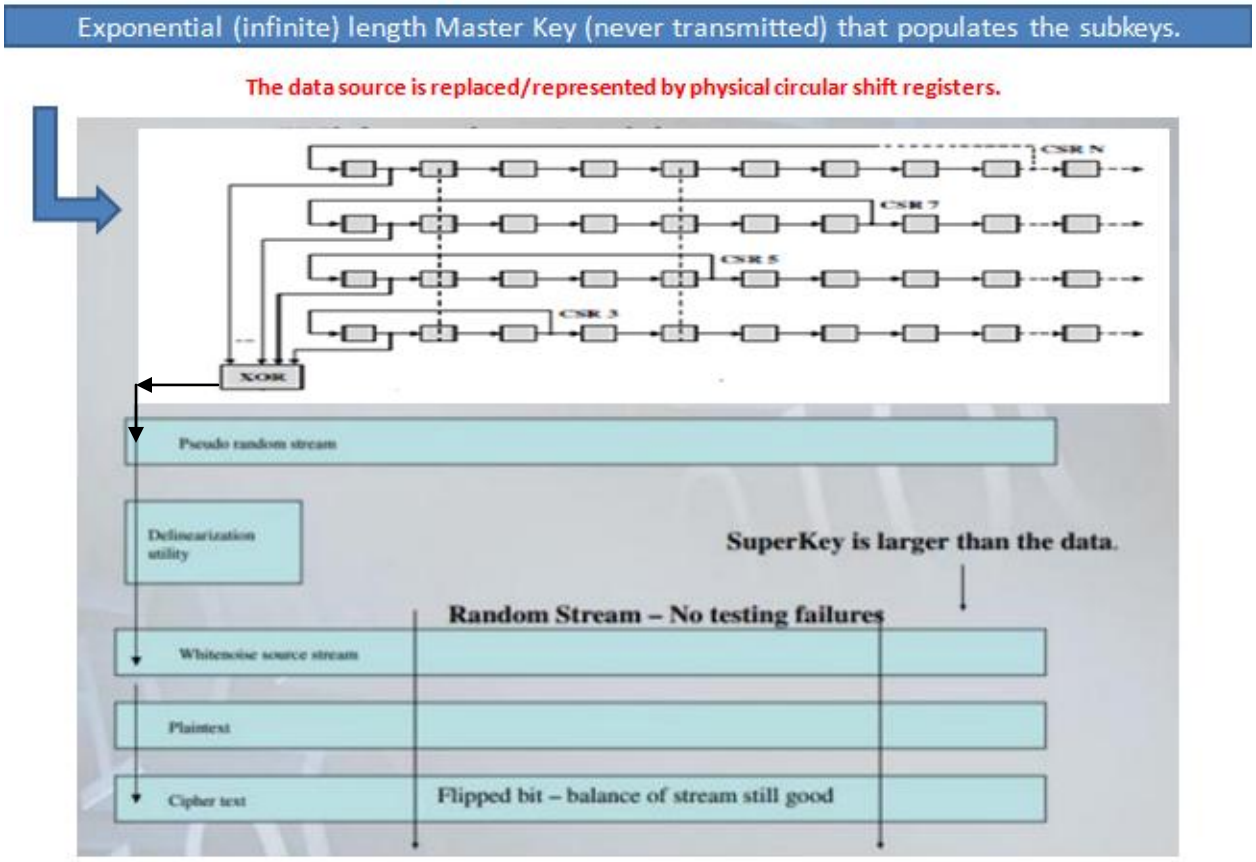
Side Channel attack

"In cryptography, a side-channel attack is any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms. For, example, timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited to break the system." wiki

In microprocessing the physical implementation may be a line feed shift register, peripheral interface controller, counters or in this case a circular shift register (CSR). Picture a combination lock on a suitcase.

We see in Figure 2 that the Master Key populates the values in the CSRs which are a physical component. The idea in trying to utilize side channel attacks against Whitenoise is that since these registers emit physical data that is theoretically available for capture that the attack bypasses or hops over the one-way-function defense that the S-Box provides in the software implementation of Whitenoise. While that appears to be a logical assumption and approach, it doesn't and cannot work for the following reasons.

Fig 2



Simple logic defense – three features that prevent side channel attacks

1. The subkey lengths (or registers) are populated with sequential, determinist, random data from a master key which has never been transmitted. Since we know that repeating the portions of the data source eliminates one-time-pad characteristics we simply insure that the registers or subkeys in physical implementations are flushed out after single use. The hacker or side channel attack has no knowledge of the master key and no ability to learn about it so when the registers are repopulated they have to start all over on a completely different problem.

2. After the subkeys or circular shift registers generate the initial key stream (labeled Pseudorandom Key Stream in both figures), two bytes are drawn from that stream, appended together, and pushed through an S-box. Two bytes entered and only one byte emerged which becomes part of the key stream that is actually used. There is no information gathered from a side channel attack on subkeys when they are represented by physical registers that can give any information of the bytes that emerge from the S-box. Remember two go in and randomly only one byte emerges for use.

3. Side channel attacks require mapping physical data against cipher text. With Whitenoise all operations are order 1 (XOr) so there is no fluctuation or pattern in the cipher text. It is like a flat line on an ECG. The attack cannot correlate the overlap between the physical data and the cipher text. It turns the attack into a brute force game and long before anything can be determined the dynamic one-time-pad key will have changed and the hacker has to keep starting over each time.

whitenoise technologies

TELECOM COUNCIL 2015 SPIFFY AWARD NOMINEE

Addendum

Office de la propriété intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An Agency of Industry Canada

BRISSON, ANDRE J.
abrisson@wnlabs.com

Date : 2015/09/09

CERTIFICAT DE DÉPÔT
FILING CERTIFICATE

N° de demande/Application No. : **2,902,587** **Date de dépôt/Filing Date** : 2015/09/01

Votre référence/ Your Reference :

Date prévue de mise à la disponibilité du public / Expected Open to Public Inspection Date : 2017/03/01

Titre de l'invention/ Title of Invention : WHITENOISE SECURE CIRCUIT DESIGN IMPLEMENTATION TECHNIQUES TO PREVENT POWER ANALYSIS ATTACKS AND OTHER SIDE CHANNEL ATTACKS, SECURE OTHER PHYSICAL CRYPTOSYSTEM IMPLEMENTATIONS, AND IMPLEMENTATION OF WHITENOISE INTO LOW COST MICRO PROCESSING AND SMART COMPONENTS ...

Demandeur(s)/Applicant(s) : BRISSON, ANDRE J.

Inventeur(s)/Inventor(s) : BRISSON, ANDRE J.