The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators

A. Theodore Markettos and Simon Moore
www.cl.cam.ac.uk/research/security

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

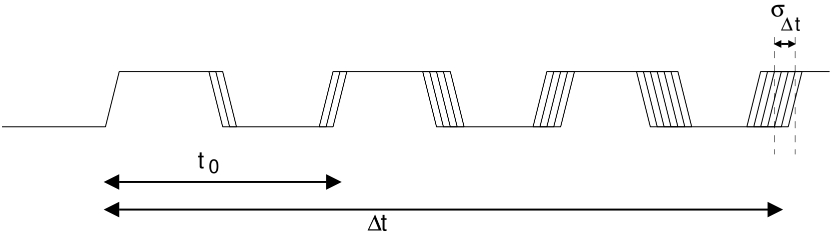
Importance of unpredictable random number generation

Many protocols are vulnerable to attacks if the random number generator (RNG) is predictable.

- Many kinds of key generation
- Replay attacks
- Digital Signature Algorithm
- Masking of RSA to protect against DPA

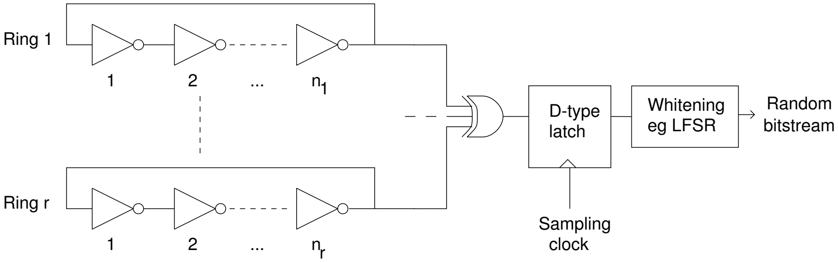
A source of randomness... jitter

- Sources of cryptographic randomness measure some physical property
- Jitter: timing variations due to noise
- Measure jitter of ring oscillators



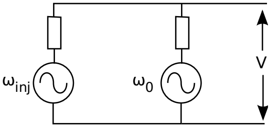
A source of randomness... jitter

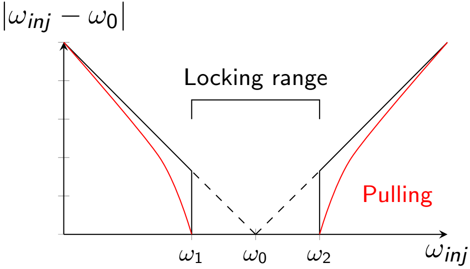
- Sources of cryptographic randomness measure some physical property
- Jitter: timing variations due to noise
- Measure jitter of ring oscillators



Injection locking

- But what happens to jitter if the ring oscillators aren't independent?
- Christiaan Huyghens, 1665: Independent pendulum clocks on a wall tend to synchronise via nonlinear vibrations through the wall
- Applying a signal near to the fundamental 'pulls-in' the oscillator to a different nearby frequency



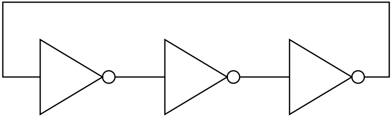


Injection locking in ring oscillators

- Ring oscillators tend to ring synchronise by parasitic injection locking
- ...so what if we try to force them to lock?
- A basic ring oscillator
- ...can have an injection signal coupled into the ring (not easy)
- A ring oscillator with power supply/EM injection is balanced
- ...unless it isn't
- ...or until an extra load is added

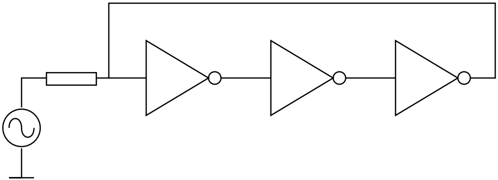
Injection locking in ring oscillators

- Ring oscillators tend to ring synchronise by parasitic injection locking
- ...so what if we try to force them to lock?
- A basic ring oscillator
- ...can have an injection signal coupled into the ring (not easy)
- A ring oscillator with power supply/EM injection is balanced
- ...unless it isn't
- ...or until an extra load is added



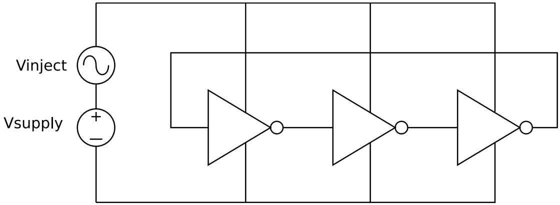
Injection locking in ring oscillators

- Ring oscillators tend to ring synchronise by parasitic injection locking
- ...so what if we try to force them to lock?
- A basic ring oscillator
- ...can have an injection signal coupled into the ring (not easy)
- A ring oscillator with power supply/EM injection is balanced
- ...unless it isn't
- ...or until an extra load is added



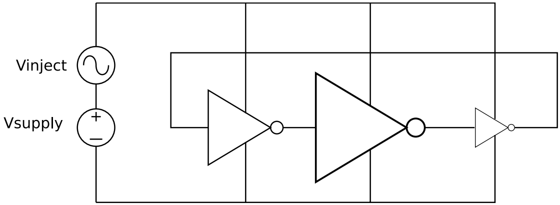
Injection locking in ring oscillators

- Ring oscillators tend to ring synchronise by parasitic injection locking
- ...so what if we try to force them to lock?
- A basic ring oscillator
- ...can have an injection signal coupled into the ring (not easy)
- A ring oscillator with power supply/EM injection is balanced
- ...unless it isn't
- ...or until an extra load is added



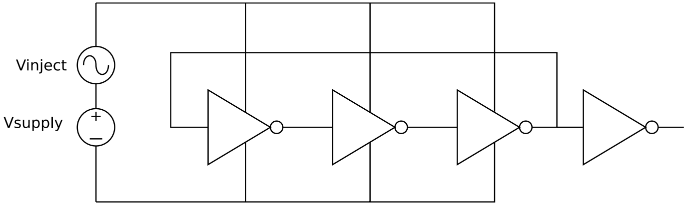
Injection locking in ring oscillators

- Ring oscillators tend to ring synchronise by parasitic injection locking
- ...so what if we try to force them to lock?
- A basic ring oscillator
- ...can have an injection signal coupled into the ring (not easy)
- A ring oscillator with power supply/EM injection is balanced
- ...unless it isn't
- ...or until an extra load is added



Injection locking in ring oscillators

- Ring oscillators tend to ring synchronise by parasitic injection locking
- ...so what if we try to force them to lock?
- A basic ring oscillator
- ...can have an injection signal coupled into the ring (not easy)
- A ring oscillator with power supply/EM injection is balanced
- ...unless it isn't
- ...or until an extra load is added



Injection locking in ring oscillators

- Ring oscillators tend to ring synchronise by parasitic injection locking
- ...so what if we try to force them to lock?
- A basic ring oscillator
- ...can have an injection signal coupled into the ring (not easy)
- A ring oscillator with power supply/EM injection is balanced
- ...unless it isn't
- ...or until an extra load is added

  - *Injection locking reduces global jitter*
  - *Injection locking of multiple rings prevents measurement of jitter differences between them*

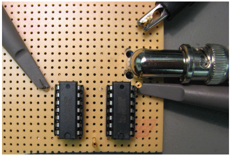
Experiment with discrete logic gates

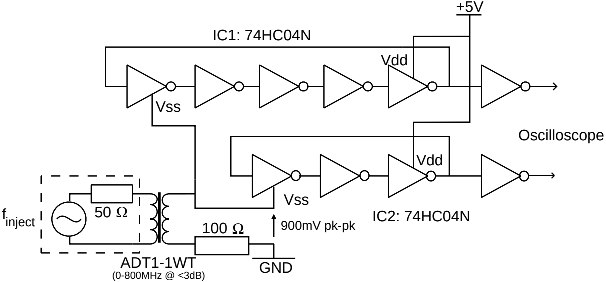
Injection locking is:

- Difficult to solve analytically
- Difficult to simulate with SPICE
- Difficult to measure inside an FPGA

So we tried some discrete logic gates:

- 74HC04 inverter, 3-element and 5-element rings, inject 24 MHz

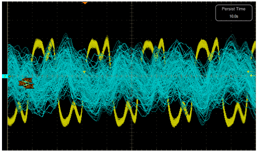




Experiment with discrete logic gates

Yellow = output of 3-element ring (trigger), blue = 5-element

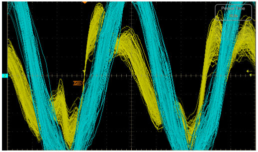
8 V



200 ns

No injection

8 V

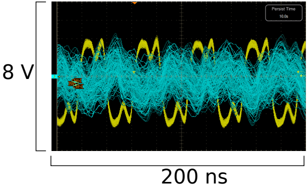


200 ns

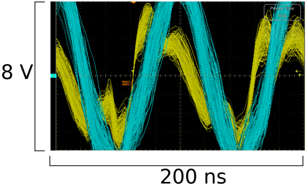
10 MHz injection at 900 mV pk-pk

Experiment with discrete logic gates

Yellow = output of 3-element ring (trigger), blue = 5-element

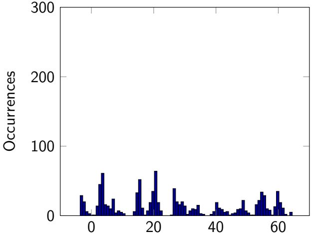


No injection

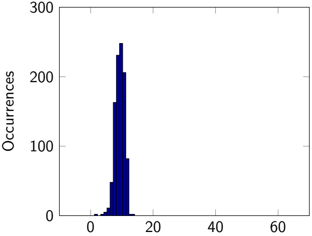


10 MHz injection at 900 mV pk-pk

Trigger on rising edge 50% of 3-element ring, measure phase lag until 50% rising of 5-element



No injection: phase lag/ns

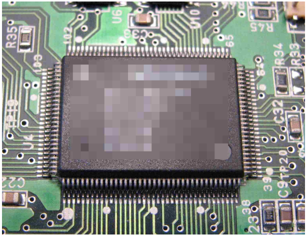


24MHz injection: phase lag/ns

ATM secure microcontroller

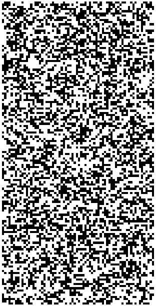
- 8051-based 8-bit microcontroller, used in ATMs
- Tamper detection, anti-probing coating, ‘the most secure’ at release
- Our example datecode 1995, still recommended for new banking applications

- TRNG from frequency differences between ring oscillators and system crystal
- 8 bits entropy every 160μs
- 64 bits make up internal key



ATM secure microcontroller

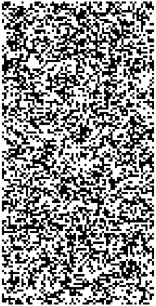
- Injected 500 mV sinusoid into 5 V power supply.
- Extract full bitstream from microcontroller. Bit patterns as rasters:



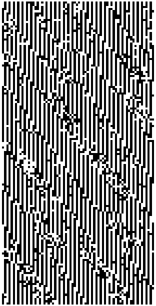
No injection

ATM secure microcontroller

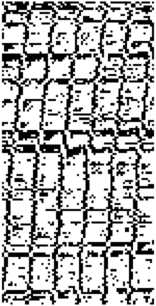
- Injected 500 mV sinusoid into 5 V power supply.
- Extract full bitstream from microcontroller. Bit patterns as rasters:



No injection

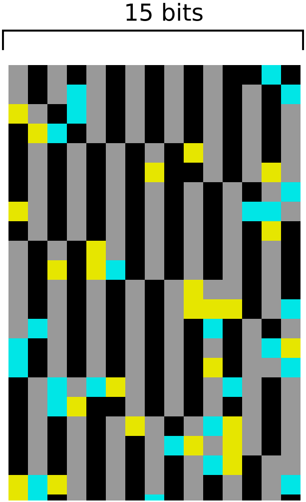


1.822880 MHz injection



1.929629 MHz injection

ATM secure microcontroller



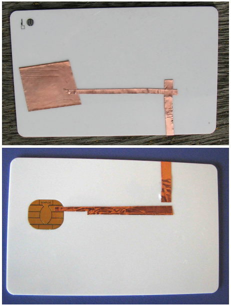
Overlaid sequences from 1.822880 MHz injection.

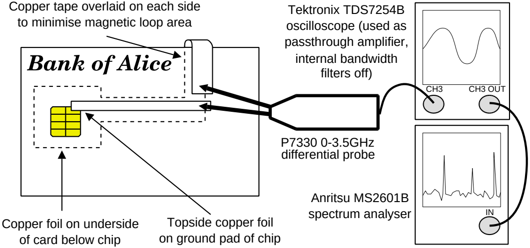
Tuples made from random bits one each from two recordings black=(0,0), grey=(1,1), yellow=(0,1), cyan=(1,0)

32 bits has not 2^{32} possible values but 225!

EMV smartcard

- EMV ('Chip and PIN') payment card from major British bank, issued 2004 (first one we picked)
- First we worked out an injection frequency using an electromagnetic attack:



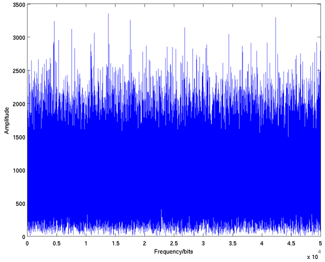


EMV smartcard

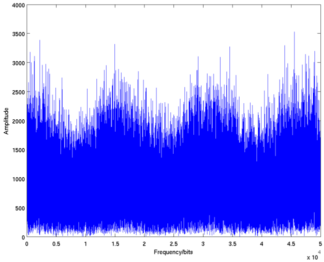
- Then we modified a card reader to inject a 1 V 24.04 MHz sinusoid into the 5 V supply
- Device still ran EMV transactions
- Read 1.6 Gbit from ISO7816 `GET_CHALLENGE` command
- Without injection, failed 1 of 188 NIST tests
- With injection, failed 160 of 188 NIST tests
- Obvious failures: 32×32 rank test, discrete Fourier transform

EMV smartcard

- Then we modified a card reader to inject a 1 V 24.04 MHz sinusoid into the 5 V supply
- Device still ran EMV transactions
- Read 1.6 Gbit from ISO7816 `GET_CHALLENGE` command
- Without injection, failed 1 of 188 NIST tests
- With injection, failed 160 of 188 NIST tests
- Obvious failures: 32×32 rank test, discrete Fourier transform



DFT, no injection



DFT, with injection.
Sequences of 2000 and 15000 bits visible.

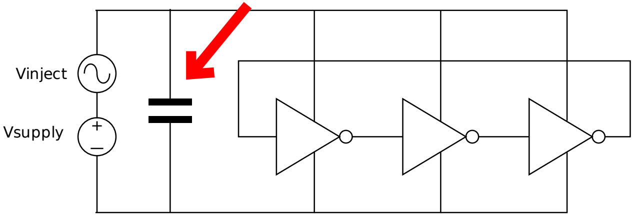
An ATM attack

- The nonce sent to an EMV smartcard used in an ATM is 32 bits
- An attacker irradiates the ATM with 10 GHz amplitude modulated with 1.8 MHz
- Ventilation slots are transparent to 10 GHz
- Device capacitance filters out the 10 GHz leaving 1.8 MHz in the power supply
- Entropy of ATM's 32 bit nonce reduced to < 8 bits (≈ 225)
- The attacker records some challenge/responses with the victim card in a modified store terminal
- A fake card is used to select the correct reply to a challenge from the irradiated ATM
- Birthday paradox: need $< \sqrt{225} = 15$ attempts for 50% chance of success (stealing money)
- Random number vulnerabilities are very difficult to detect or prove

Defences

Similar to DPA defences:

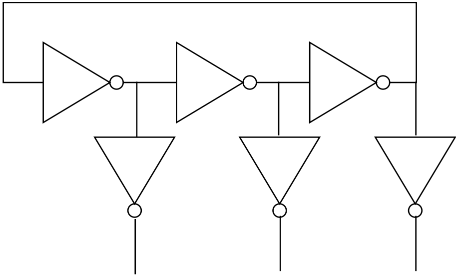
- Power supply filtering
- Balanced rings
- Differential ring oscillator (ie dual rail)



Defences

Similar to DPA defences:

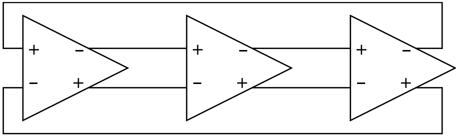
- Power supply filtering
- Balanced rings
- Differential ring oscillator (ie dual rail)



Defences

Similar to DPA defences:

- Power supply filtering
- Balanced rings
- Differential ring oscillator (ie dual rail)



Defences

Similar to DPA defences:

- Power supply filtering
- Balanced rings
- Differential ring oscillator (ie dual rail)

But won't our smartcard already have DPA protection?

Summary

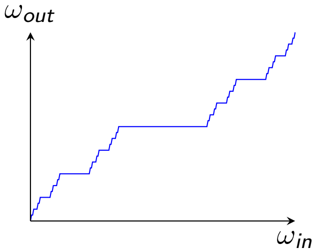
- Injection locking is well-known as a parasitic effect
- We have extended it to an attack
- The attack is straightforward to implement
- The attack works surprisingly well

Questions?

The Security Group:

- blog:
  `http://www.lightbluetouchpaper.org`
- webpage:
  `http://www.cl.cam.ac.uk/research/security`

Injection locking



The "Devil's Staircase"