Distinguishing iterated encryption

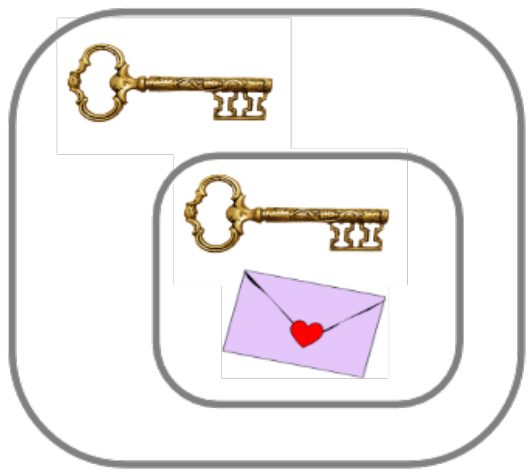
E. Lambooij
eran@hideinplainsight.io

This is joint work with:
Orr Dunkelman, Nathan Keller and Tanja Lange

CRYPTACUS Workshop, 16-18 November 2017

Question:

Does security increase if we encrypt twice with the same key? And thrice? And four times? And what about encrypting it t times with the same key?



Distinguishing t-encryption

We can view an encryption under key k as a permutation:

$$E_k \in \mathcal{P}$$

Then double encryption can be viewed as a squared permutation:

$$E_k(E_k(p)) = E_k^2(p) \in \mathcal{P}^2$$

Question, can we distinguish:

$$p \text{ from } (p')^2 \text{ with } p, p' \in \mathcal{P}$$

Or even more interesting:

$$p \text{ from } (p')^2 \text{ with } p, p' \in \mathcal{P}_{\text{even}}$$

Permutation basics

Let the permutation σ be defined as:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 2 & 8 & 9 & 4 & 7 & 10 & 5 & 1 & 6 \end{pmatrix}$$

Permutation basics

Let the permutation σ be defined as:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 2 & 8 & 9 & 4 & 7 & 10 & 5 & 1 & 6 \end{pmatrix}$$

The disjoint cycle decomposition of σ is:

$$\sigma = (1, 3, 8, 5, 4, 9)(2)(6, 7, 10)$$

Permutation basics

Let the permutation σ be defined as:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 2 & 8 & 9 & 4 & 7 & 10 & 5 & 1 & 6 \end{pmatrix}$$

The disjoint cycle decomposition of σ is:

$$\sigma = (1, 3, 8, 5, 4, 9)(2)(6, 7, 10)$$

Squaring σ gives:

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 2 & 5 & 1 & 9 & 7 & 10 & 4 & 3 & 6 \end{pmatrix}$$

Permutation basics

Let the permutation σ be defined as:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 2 & 8 & 9 & 4 & 7 & 10 & 5 & 1 & 6 \end{pmatrix}$$

The disjoint cycle decomposition of σ is:

$$\sigma = (1, 3, 8, 5, 4, 9)(2)(6, 7, 10)$$

Squaring σ gives:

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 2 & 5 & 1 & 9 & 7 & 10 & 4 & 3 & 6 \end{pmatrix}$$

The disjoint cycle decomposition of σ^2 is:

$$\sigma^2 = (1, 8, 4)(3, 5, 9)(2)(6, 7, 10)$$

Distinguishing t-encryption

σ^t splits all cycles with length divisible by t up into t equally sized cycles.

Distinguishing t-encryption

σ^t splits all cycles with length divisible by t up into t equally sized cycles.

$$E(\#\text{cycles in } \sigma^t) \geq E(\#\text{cycles in } \sigma')$$

Distinguishing t-encryption

σ^t splits all cycles with length divisible by t up into t equally sized cycles.

$$E(\#\text{cycles in } \sigma^t) \geq E(\#\text{cycles in } \sigma')$$

Given a random permutation σ

$$E(\#\text{cycles in } \sigma) = \sum_{m=1}^{N} \frac{1}{m} = H_N \approx \ln N$$

Distinguishing t-encryption

σ^t splits all cycles with length divisible by t up into t equally sized cycles.

$$E(\#\text{cycles in } \sigma^t) \geq E(\#\text{cycles in } \sigma')$$

Given a random permutation σ

$$E(\#\text{cycles in } \sigma) = \sum_{m=1}^{N} \frac{1}{m} = H_N \approx \ln N$$

Given a random permutation σ, and t is prime

$$E(\#\text{cycles in } \sigma^t) \approx \frac{2t-1}{t} \ln N$$

Distinguishing t-encryption

σ^t splits all cycles with length divisible by t up into t equally sized cycles.

$$E(\#\text{cycles in } \sigma^t) \geq E(\#\text{cycles in } \sigma')$$

Given a random permutation σ

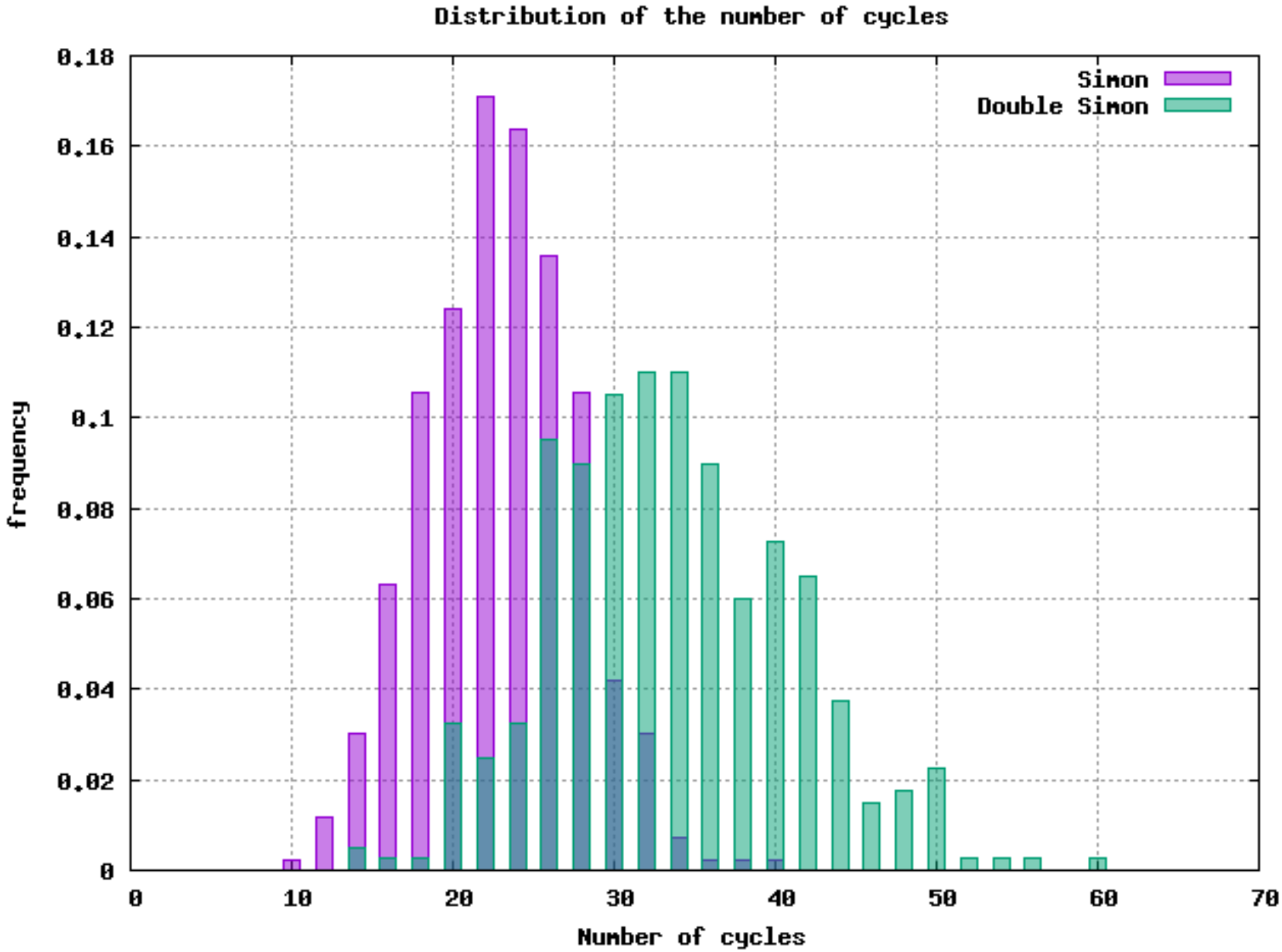
$$E(\#\text{cycles in } \sigma) = \sum_{m=1}^{N} \frac{1}{m} = H_N \approx \ln N$$

Given a random permutation σ, and t is prime

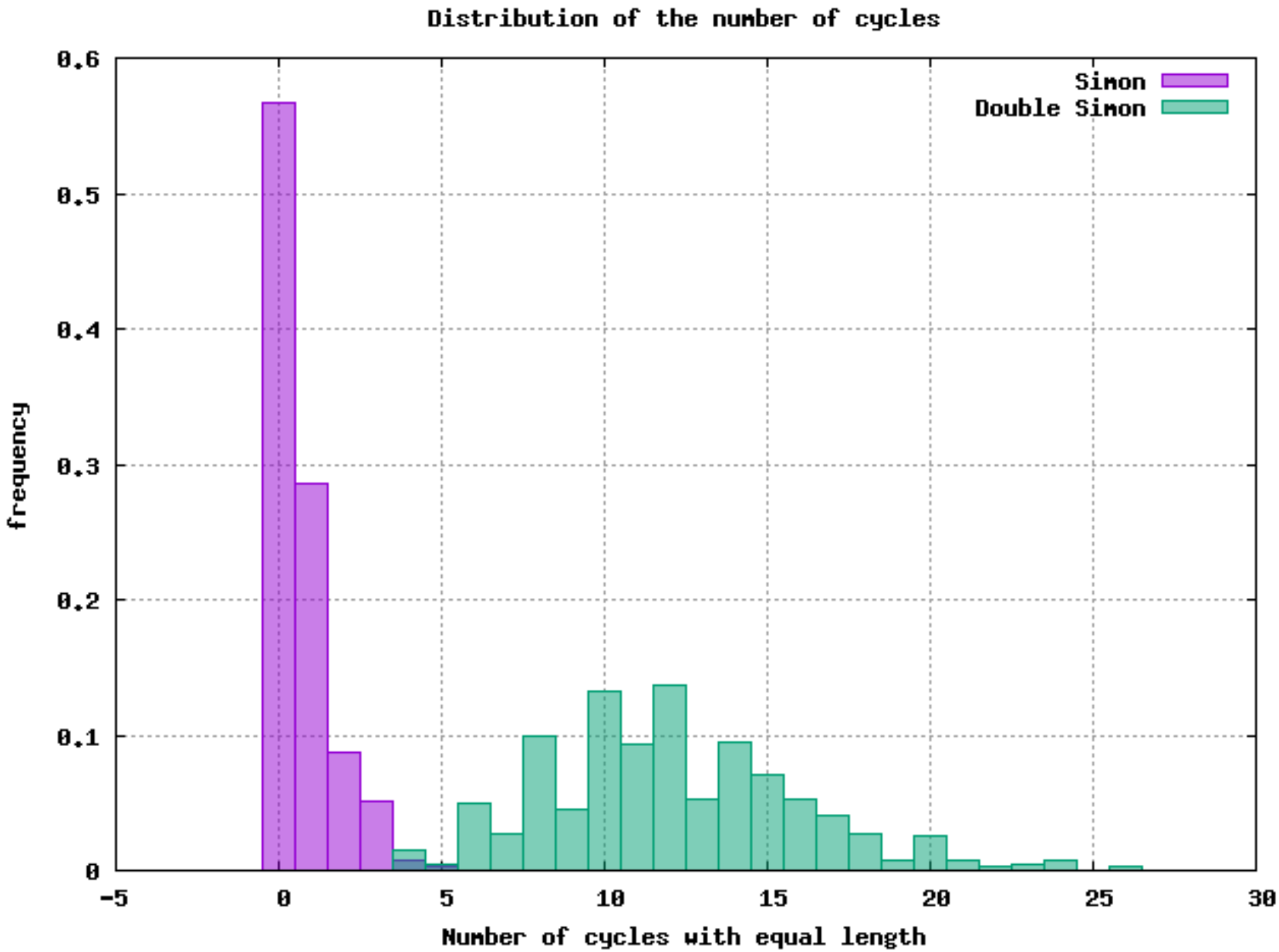
$$E(\#\text{cycles in } \sigma^t) \approx \frac{2t-1}{t} \ln N$$

$$E(\#\text{cycles split in } \sigma^t) \approx \frac{\ln N}{t}$$

Experiment


Distribution of the number of cycles
Simon
Double Simon
frequency
0.18
0.16
0.14
0.12
0.1
0.08
0.06
0.04
0.02
0
0
10
20
30
40
50
60
70
Number of cycles

Experiment (2)



Distinguishers

- Three distinguishers
- All have (near) full codebook data complexity

Distribution distinguisher

- Based on the difference in expected number of cycles
- The number of cycles in a permutation of size n has an expected number of cycles of $\ln n$
- The number of cycles in a permutation to a prime power of t has an expected number of cycles of $\frac{2t-1}{t} \ln n$
- With $t = 2$, if the permutation contains more than $1.233 \cdot \ln n$ cycles it is a squared (or higher order) permutation.

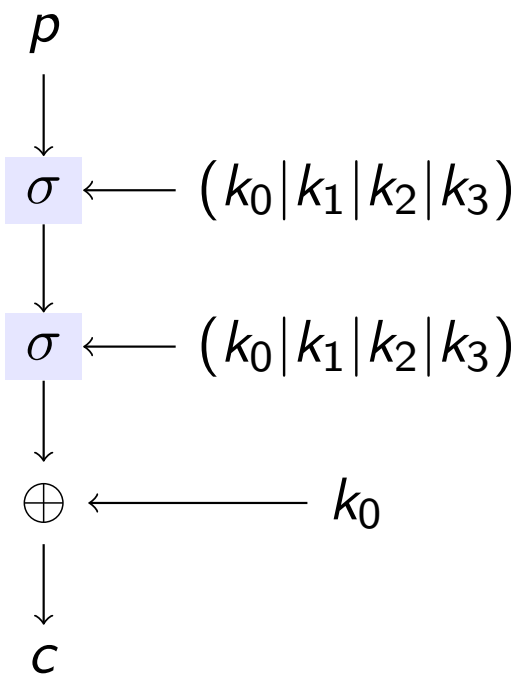
Equal cycle length distinguisher

- The probability of two cycles in a random permutation having the same length is $\frac{1}{m^2}$
- Thus finding two decently large cycles with the same size is a good que for having a squared (or higher power) permutation.

Impossible cycle length distinguisher

- In a squared permutation of size n no cycles with length $> \frac{n}{2}$ and an even cylce length are possible.
- The probability of a cycle having even length and length $> \frac{n}{2}$ is 0.1732...
- This can be used as a distinguisher.

Attacking an encryption scheme



- Take a block cipher E_κ with key $\kappa = k_0|k_1|k_2|k_3$, and blocksize b.
- Note that $\sigma^t \oplus A$ cannot be disinguished from a random even permutation, but σ^t can be distinguished.
- This means that the block cipher can be broken with $O(2^b)$ data and $O(2^{b+|A|})$ computations (with the current distinguishers).
- In this case lets take $b = 64$ and $|\kappa| = 128$, then we need 2^{64} data and 2^{64} computations to recover k_0 and 2^{96} computations to recover the remainder $k_1|k_2|k_3$. So a total of 2^{64} data and 2^{96} computations.

The attack

1. Collect data $(O(2^b))$
2. For every possible subkey A: $(O(2^{|k_0|})$
   - 2.1 XOR all ciphertexts with A $(O(2^b))$
   - 2.2 If data behaves as a squared permutation $k_0 = A$, else continue $(O(2^b))$
3. Brute force the remaining subkeys

Conclusion

- Similar applicability as slide attacks, worse but more general
- Attack complexity determined by the size of a permutation
- Round constants are a good counter measure
- Attack complexity can get significantly better with a better distinguisher

Thank you for your attention