Cryptography
Research
Centre

Randomness Testing of the NIST Light Weight Cipher Finalist Candidates

Lightweight Cryptography Workshop 2022

Emanuele Bellini, Yun Ju Huang @ TII

Technology
Innovation
Institute

Contribution

- Propose a randomness test to all possible reduced rounds of the underlying primitives of NIST LW cipher candidates to analyze their randomness level.
- Make observation of these underlying primitives and provide a metric to compare how conservative is the choice of the number of rounds in each candidate.

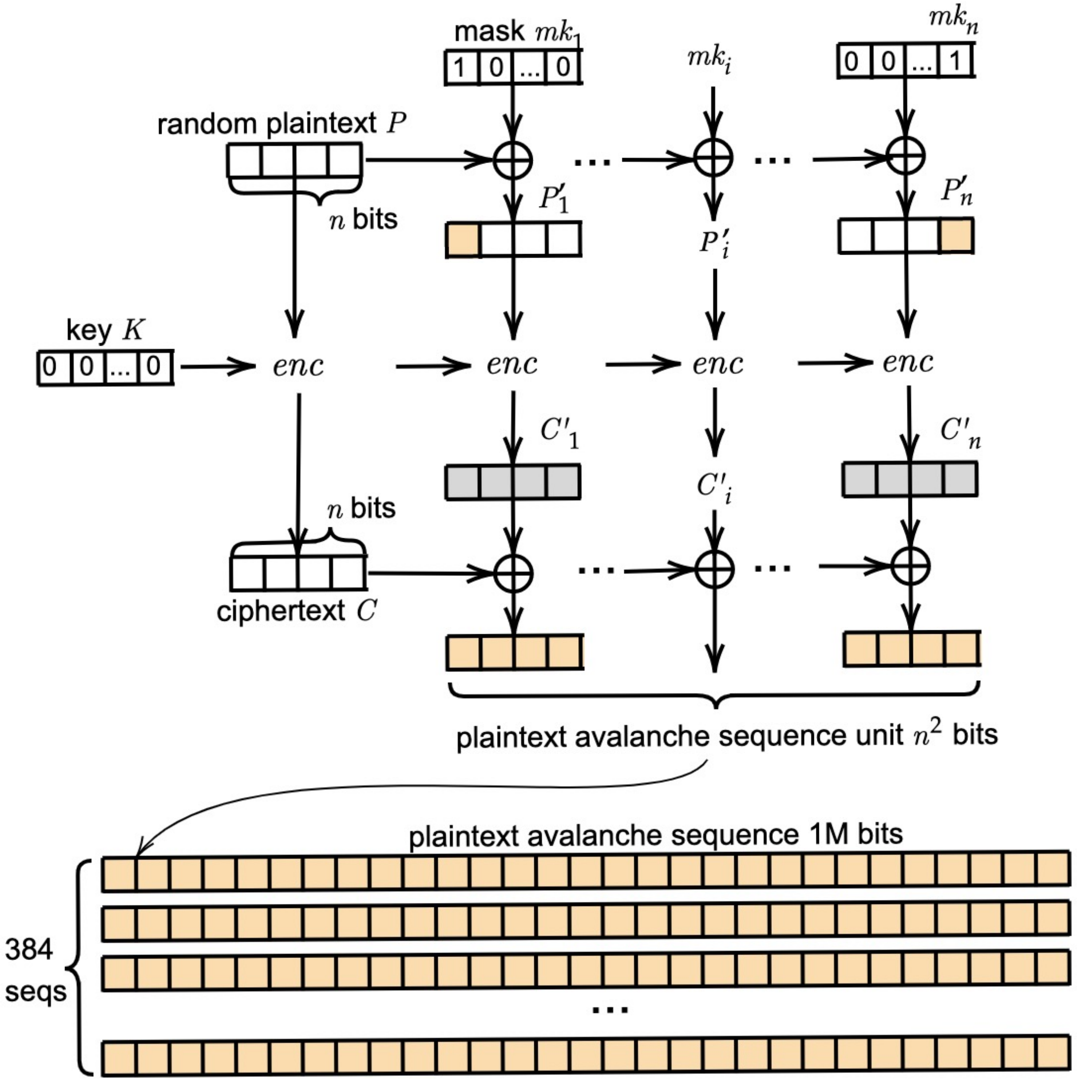
Related Works - AES

NIST released the analysis of the Advanced Encryption Standard candidate algorithms with respect to some statistical properties in 2000. [Sot99 , BS00]

Cryptography Research Centre

Experiments Setup

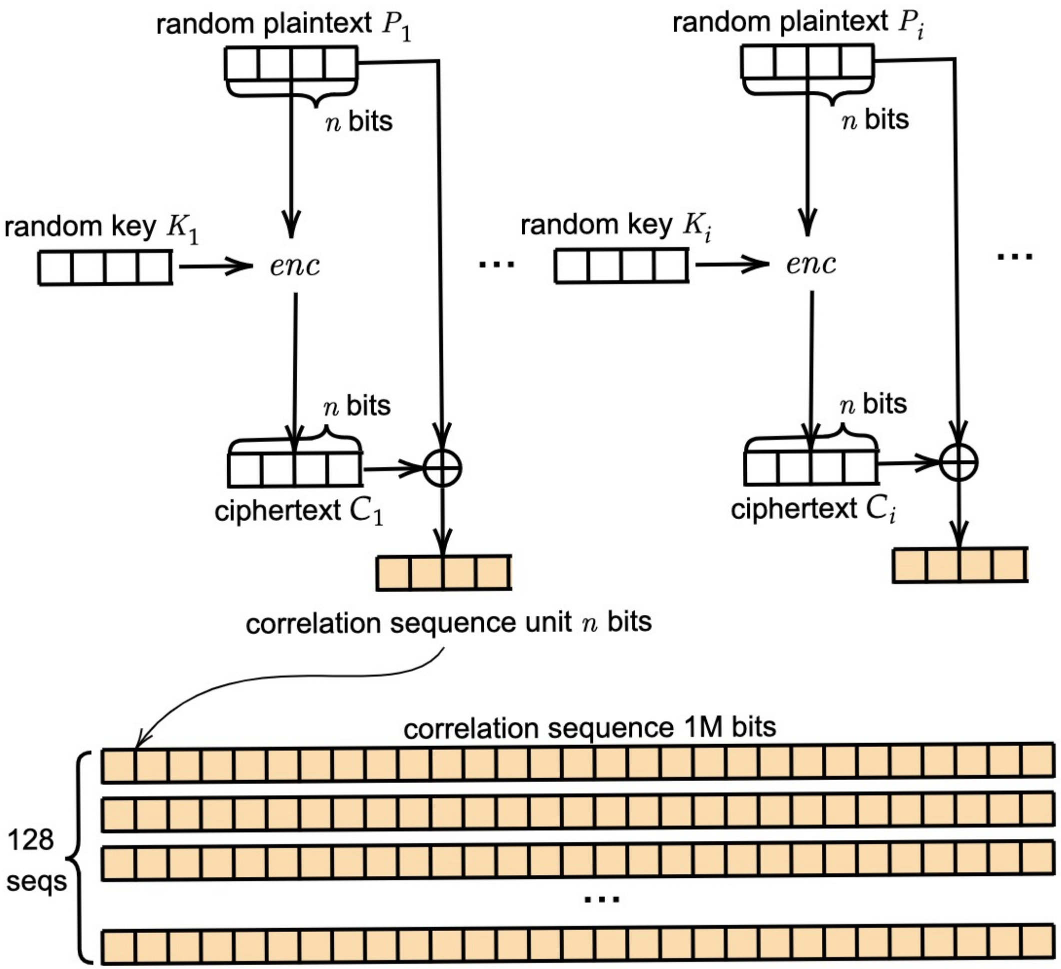
Data generation



1. **Avalanche Plaintext**
2. **Avalanche Key**
3. Plaintext-Ciphertext correlation
4. Cipher Block Chaining Mode
5. Random
6. Low-Density with Plaintext
7. Low-Density with Key
8. High-Density with Plaintext
9. High-Density with Key

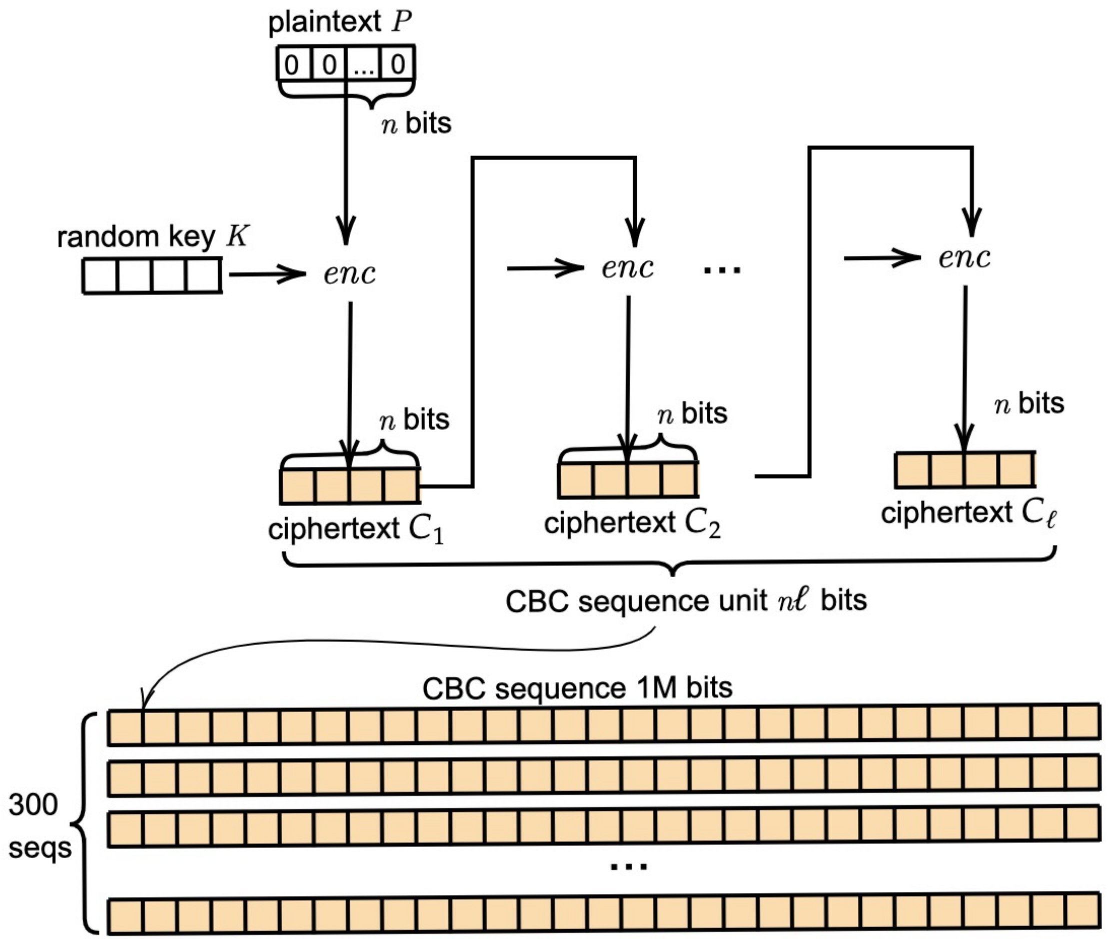
Experiments Setup

Data generation



1. Avalanche Plaintext
2. Avalanche Key
3. **Plaintext-Ciphertext correlation**
4. Cipher Block Chaining Mode
5. Random
6. Low-Density with Plaintext
7. Low-Density with Key
8. High-Density with Plaintext
9. High-Density with Key

Cryptography Research Centre



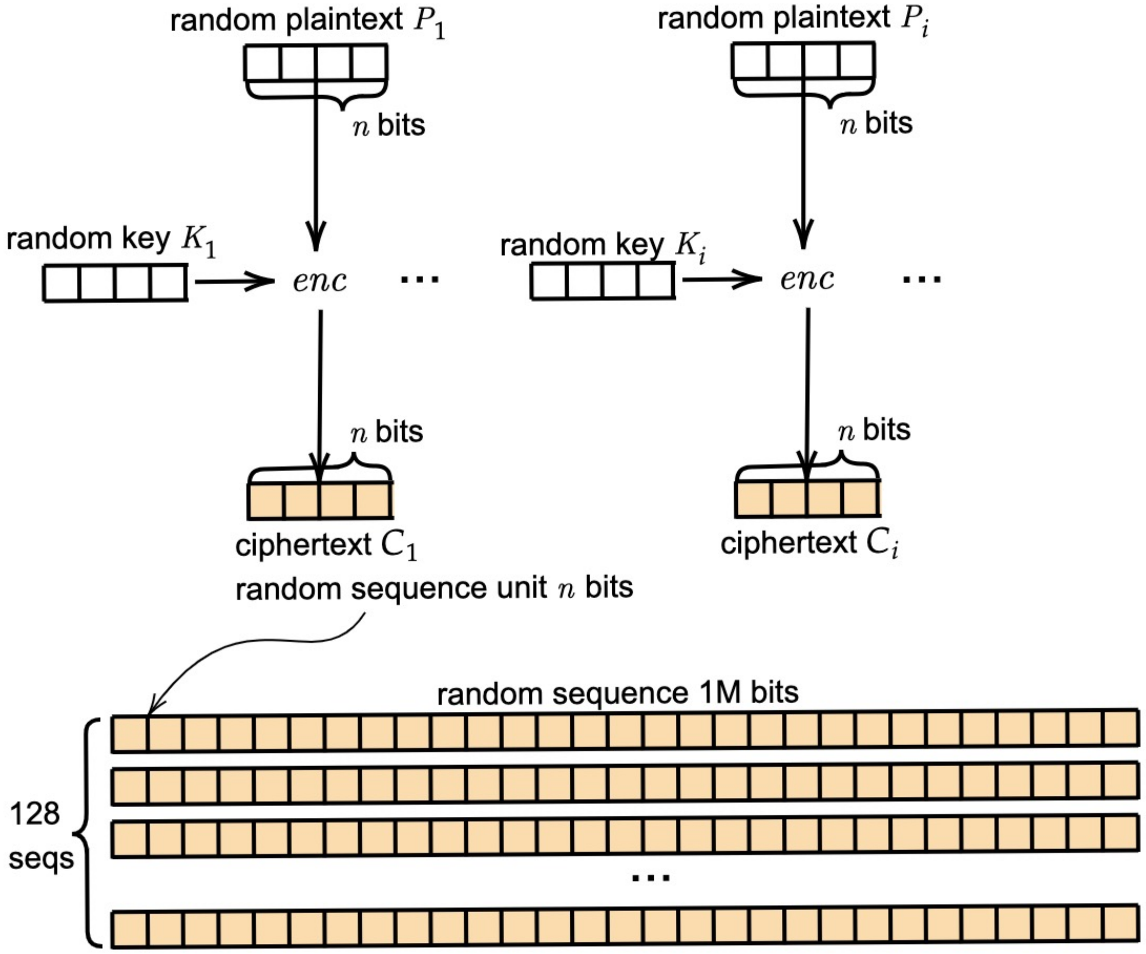
Experiments Setup

Data generation

1. Avalanche Plaintext
2. Avalanche Key
3. Plaintext-Ciphertext correlation
4. **Cipher Block Chaining Mode**
5. Random
6. Low-Density with Plaintext
7. Low-Density with Key
8. High-Density with Plaintext
9. High-Density with Key

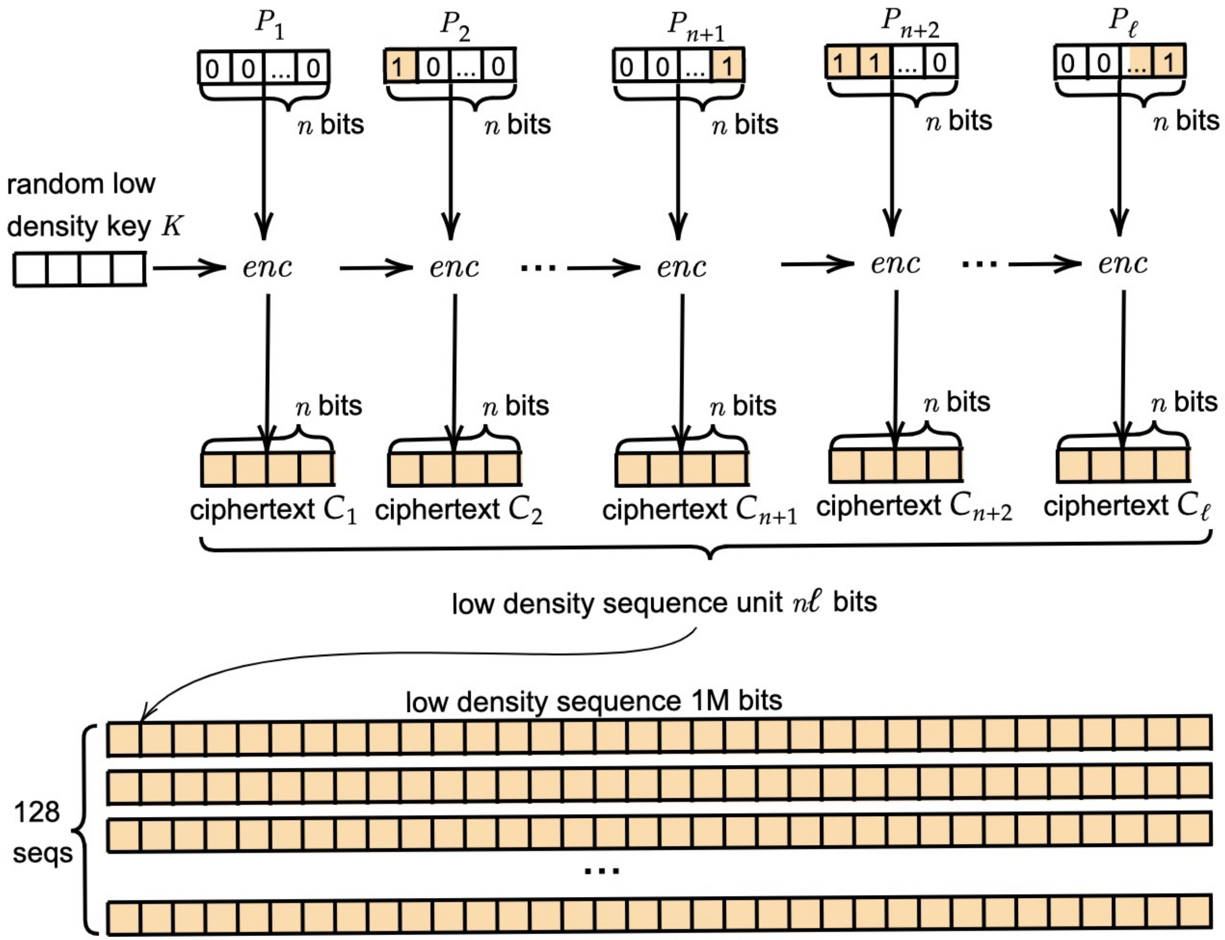
Experiments Setup

Data generation



1. Avalanche Plaintext
2. Avalanche Key
3. Plaintext-Ciphertext correlation
4. Cipher Block Chaining Mode
5. **Random**
6. Low-Density with Plaintext
7. Low-Density with Key
8. High-Density with Plaintext
9. High-Density with Key

Experiments Setup



Data generation

1. Avalanche Plaintext
2. Avalanche Key
3. Plaintext-Ciphertext correlation
4. Cipher Block Chaining Mode
5. Random
6. **Low-Density with Plaintext**
7. **Low-Density with Key**
8. **High-Density with Plaintext**
9. **High-Density with Key**

Experiments Setup

NIST Statistical Tools

Using the tools provided on the NIST website

https://csrc.nist.gov/Projects/Random-Bit-Generation/Documentation-and-Software

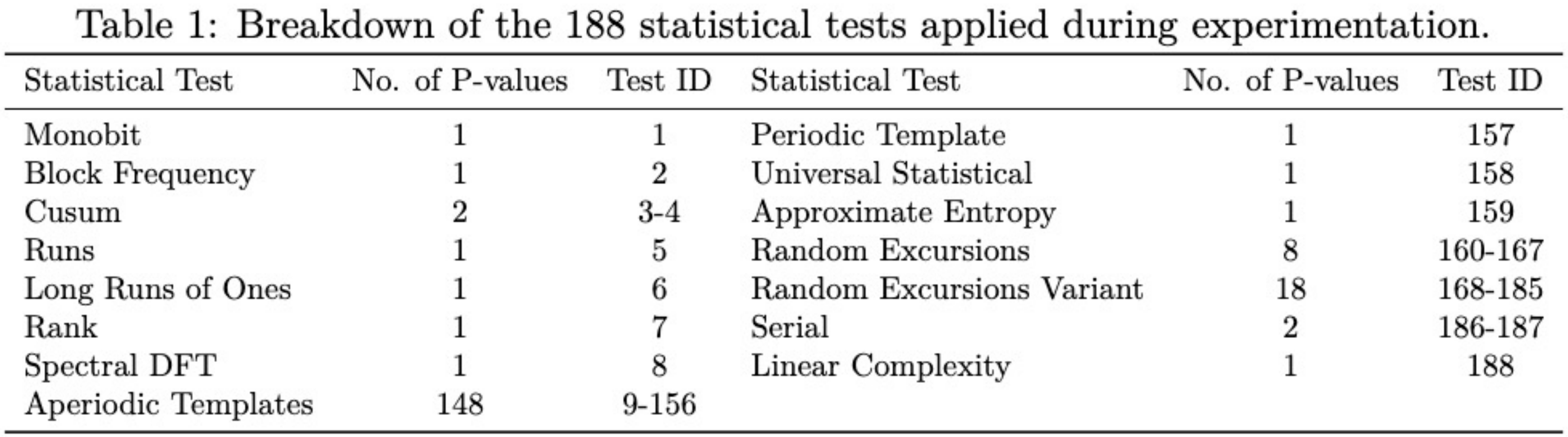


Table 1: Breakdown of the 188 statistical tests applied during experimentation.

Statistical Test	No. of P-values	Test ID	Statistical Test	No. of P-values	Test ID
Monobit	1	1	Periodic Template	1	157
Block Frequency	1	2	Universal Statistical	1	158
Cusum	2	3-4	Approximate Entropy	1	159
Runs	1	5	Random Excursions	8	160-167
Long Runs of Ones	1	6	Random Excursions Variant	18	168-185
Rank	1	7	Serial	2	186-187
Spectral DFT	1	8	Linear Complexity	1	188
Aperiodic Templates	148	9-156			

Experiments Setup

Environment

- Currently, we generated total around 462 GB datasets for the test.
- The executing time of current result is 1 month.
- Running environment
  - Server 1 and 2: 16 Intel(R) Xeon(R) Gold 5222 CPUs, 4-cores, 3.80GHz, 252G RAM
  - Server 3: 112 Intel(R) Xeon(R) Platinum 8280 CPUs, 28-cores, 2.70GHz, 1152G RAM
- The dataset generation has been performed using the NumPy library and an independent non-optimized python implementation of each cipher.
- GRAIN-128 is excluded.
- CBC data of Spongent-pi is excluded.

Randomness Test Results

NIST LW cipher	Underlying Primitives Permutation	Block Size	Key Size	Avalanche	
				Plaintext	Key
SPN-based Permutation					
Ascon	Ascon's Permutation	320	–	4|[6,12]	–
Elephant	Dumbo: Elephant-Spongent-π[160]	160	–	8|80	–
	Jumbo: Elephant-Spongent-π[176]	176	–	8|90	–
	Delirium: Elephant-Keccak-f[200]	200	–	3|18	–
ISAP	Ascon's Permutation	320	–	4|[1,12]	–
	Keccak-p[400]	400	–	3|[1,20]	–
PHOTON-Beetle	PHOTON256	256	–	3|12	–
Xoodyak	Xoodoo	384	–	4|12	–
SPARKLE (SCHWAEMM and ESCH)	Sparkle256*ns*	256	–	3|[7,10]	–
	Sparkle384*ns*	384	–	3|[7,11]	–
	Sparkle512*ns*	521	–	3|[8,12]	–
Keyed Permutation					
TinyJambu	TinyJambu-128 P1024	128	128	17|[20,32]	19|[20,32]
	TinyJambu-192 P1152	128	192	17|[20,36]	21|[20,36]
	TinyJambu-256 P1280	128	256	17|[20,40]	23|[20,40]
SPN-based Block Cipher					
GIFT-COFB	GIFT-128	128	128	8|40	10|40
Tweakable Block Cipher					
Romulus	skinny-128-384+	128	384	7|40	8|40

Randomness Test Results

NIST LW cipher	Underlying Primitives Permutation	Block Size	Key Size	Plaintext/Ciphertext Correlation	CBC	Random
SPN-based Permutation						
Ascon	Ascon's Permutation	320	-	1|[6,12]	1|[6,12]	1|[6,12]
Elephant	Dumbo: Elephant-Spongent-π[160]	160	-	1|80	-	1|80
	Jumbo: Elephant-Spongent-π[176]	176	-	1|90	-	1|90
	Delirium: Elephant-Keccak-f[200]	200	-	1|18	1|18	1|18
ISAP	Ascon's Permutation	320	-	1|[1,12]	1|[1,12]	1|[1,12]
	Keccak-p[400]	400	-	1|[1,20]	1|[1,20]	1|[1,20]
PHOTON-Beetle	PHOTON256	256	-	1|12	1|12	1|12
Xoodyak	Xoodoo	384	-	1|12	1|12	1|12
SPARKLE (SCHWAEMM and ESCH)	Sparkle256*ns*	256	-	1|[7,10]	1|[7,10]	1|[7,10]
	Sparkle384*ns*	384	-	1|[7,11]	1|[7,11]	1|[7,11]
	Sparkle512*ns*	512	-	1|[8,12]	1|[8,12]	1|[8,12]
Keyed Permutation						
TinyJambu	TinyJambu-128 P1024	128	128	4|[20,32]	4|[20,32]	1|[20,32]
	TinyJambu-192 P1152	128	192	4|[20,36]	4|[20,36]	1|[20,36]
	TinyJambu-256 P1280	128	256	4|[20,40]	4|[20,40]	1|[20,40]
SPN-based Block Cipher						
GIFT-COFB	GIFT-128	128	128	2|40	2|40	1|40
Tweakable Block Cipher						
Romulus	skinny-128-384+	128	384	1|40	1|40	1|40

Randomness Test Results

NIST LW cipher	Underlying Primitives Permutation	Block Size	Key Size	Low Density		High Density	
				Plaintext	Key	Plaintext	Key
SPN-based Permutation							
Ascon	Ascon's Permutation	320	–	–	–	–	–
Elephant	Dumbo: Elephant-Spongent-π[160]	160	–	–	–	–	–
	Jumbo: Elephant-Spongent-π[176]	176	–	–	–	–	–
	Delirium: Elephant-Keccak-f[200]	200	–	–	–	–	–
ISAP	Ascon's Permutation	320	–	–	–	–	–
	Keccak-p[400]	400	–	–	–	–	–
PHOTON-Beetle	PHOTON256	256	–	–	–	–	–
Xoodyak	Xoodoo	384	–	–	–	–	–
SPARKLE (SCHWAEMM and ESCH)	Sparkle256*ns*	256	–	–	–	–	–
	Sparkle384*ns*	384	–	–	–	–	–
	Sparkle512*ns*	512	–	–	–	–	–
Keyed Permutation							
TinyJambu	TinyJambu-128 P1024	128	128	14|[20,32]	17|[20,32]	14|[20,32]	17|[20,32]
	TinyJambu-192 P1152	128	192	14|[20,36]	17|[20,36]	14|[20,36]	17|[20,36]
	TinyJambu-256 P1280	128	256	15|[20,40]	19|[20,40]	14|[20,40]	20|[20,40]
SPN-based Block Cipher							
GIFT-COFB	GIFT-128	128	128	7|40	9|40	7|40	8|40
Tweakable Block Cipher							
Romulus	skinny-128-384+	128	384	6|40	8|40	6|40	8|40

Conclusion

We can see that most of the underlying primitives produce datasets which seem random in the first third of the total number of rounds. For the Spongent-pi this proportion is much higher, which seems to indicate a very conservative choice in the number of rounds of this cipher. Also, the schemes which using block ciphers as the underlying primitives also have parameter with higher rounds.

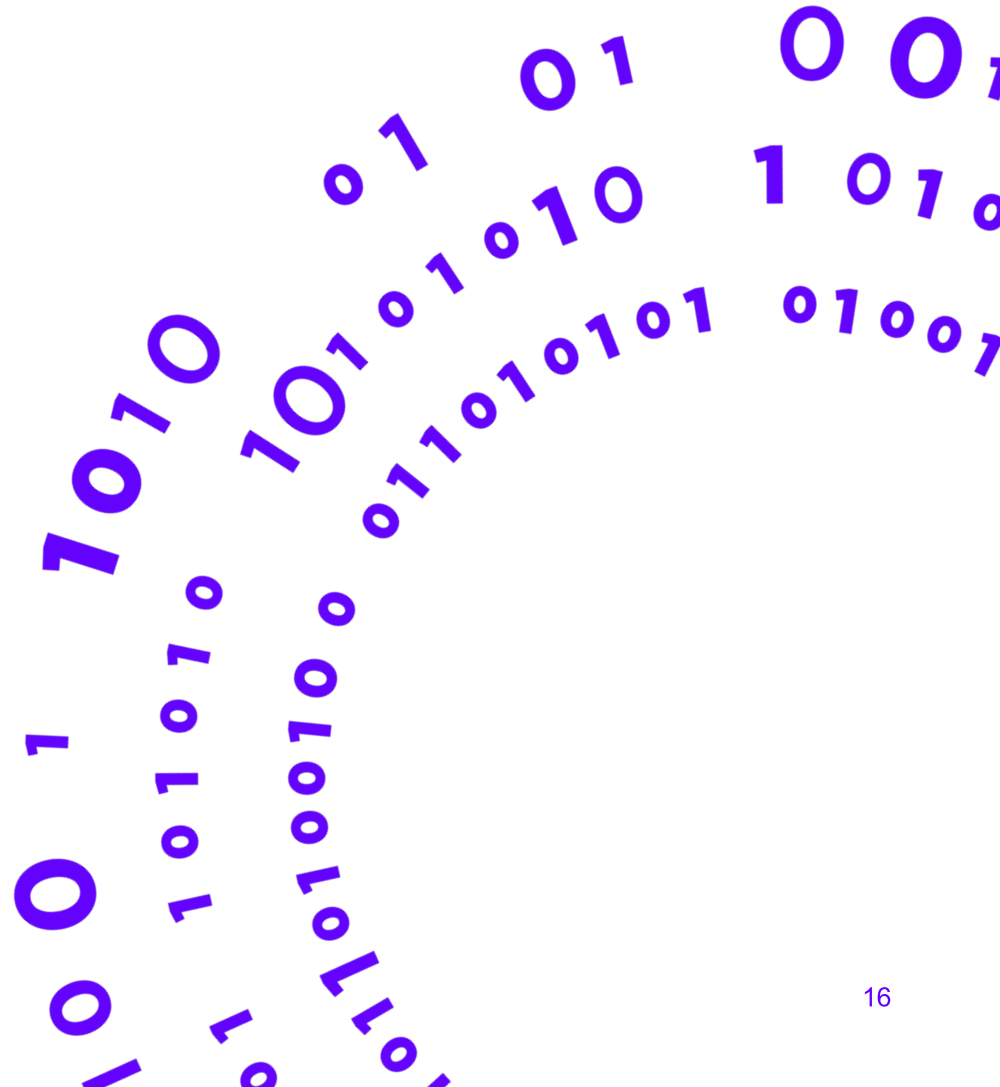
In some scheme, different rounds of the underlying primitives are used. Ascon and Sparkle family choose this parameters in more conservative way. On the other hand, we can see that in some cipher like ISAP and TinyJambu seems more aggressive to have some none random choice when doing the small task such as initialization or metadata encryption.

Reference

- [Sot99] Juan Soto. NISTIR 6390: Randomness testing of the advanced encryption standard candidate algorithms. NIST Internal or Interagency Reports, 1999
- [BS00] Lawrence Bassham and Juan Soto. NISTIR 6483: Randomness testing of the advanced encryption standard finalist candidates. NIST Internal or Interagency Reports, 2000.

For more details, please refer to the paper.

Q & A



TII Technology Innovation Institute

Cryptography Research Centre

tii.ae