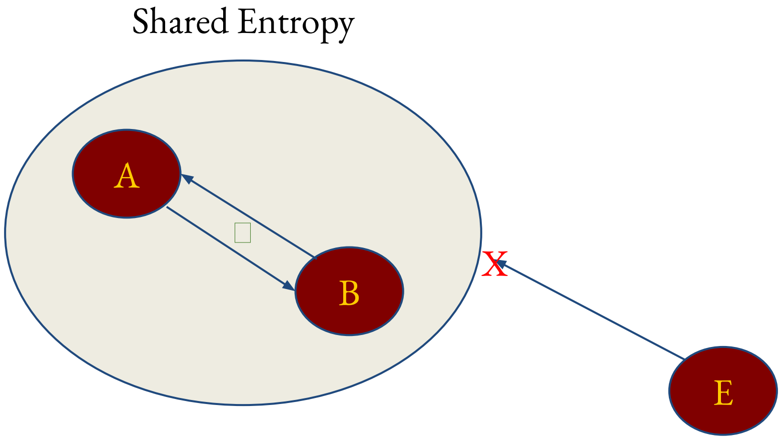
IPSN 2021

Moonshine: An Online Randomness Distiller for Zero-Involvement Authentication

Jack West, *Kyuin Lee, Suman Banerjee, Younghyun Kim, George K. Thiruvathukal, Neil Klingensmith*

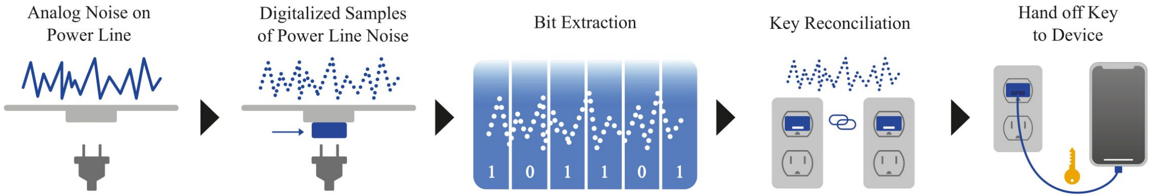
LOYOLA
UNIVERSITY CHICAGO
AD · MAJOREM · DEI · GLORIAM
1870

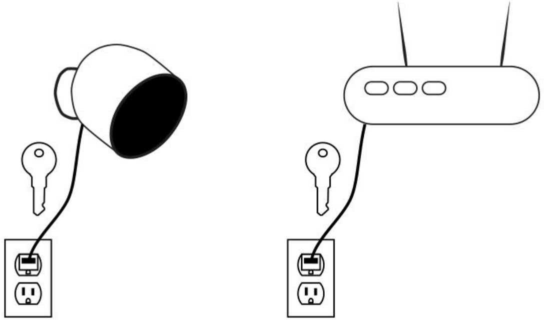
Zero-Involvement Authentication (ZIA)

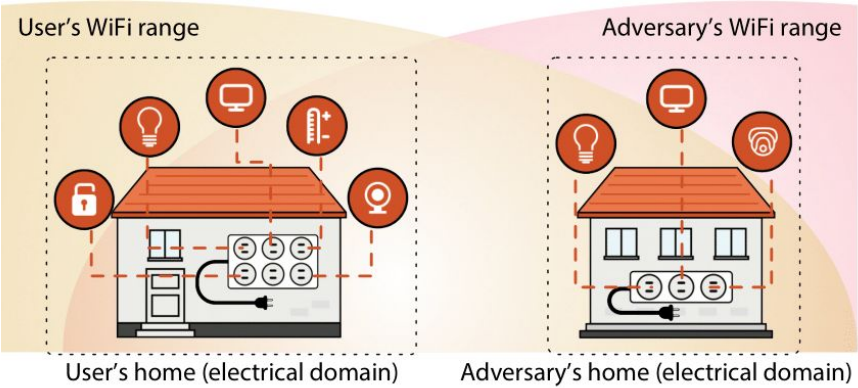


- **Minimal Communication Security Scheme**
- **Relies on a locally shared entropy source**
- **Great for scalable independent IoT systems**

VoltKey


Analog Noise on Power Line
Digitalized Samples of Power Line Noise
Bit Extraction
1 0 1 1 0 1
Key Reconciliation
Hand off Key to Device




User's WiFi range
Adversary's WiFi range
User's home (electrical domain)
Adversary's home (electrical domain)

ZIA Examples

Entropy Source	Feature
Electrocardiogram	Authentication to a patient’s wearables devices in emergency situations
Shaking two devices simultaneously	Fast context-based authentication
Received Signal Strength (RSS)	Stationary proximity based authentication
Ambient Audio	Context-based authentication

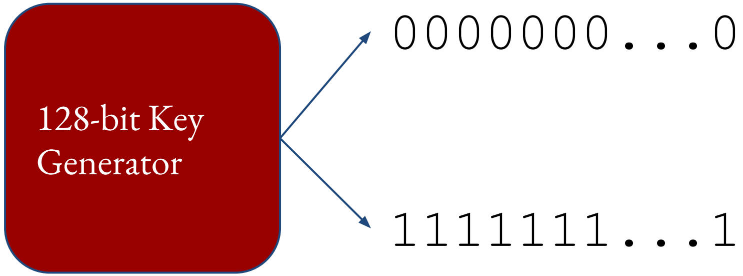
ZIA Schemes are based on contextual sources that two devices share

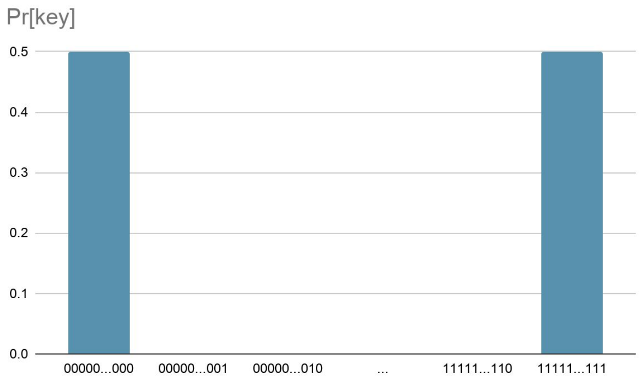
WHAT MAKES A GOOD KEY?

128-bit Key Generator → 0110100001...

2^{128} Possible Combinations

WHAT MAKES A GOOD KEY?





~~2^{128} Possible Combinations~~

2 Combinations

WHAT MAKES A GOOD KEY?

~~2^{128} Possible Combinations~~

2 Combinations

NIST Test Suite Evaluation

	Pass Rate	Frequency	Block Frequency	Cumulative Sums Fwd	Cumulative Sums Rev	Runs	Longest Run	Rank	FFT	Non-Overlap Template	Overlap Template	Universal	Approx. Entropy	Serial	Serial	Linear Complexity
Jana et al.	10/15	☐	☐	☐	☐	☐	☐		☐				☐	☐	☐	
H2B	8/15	☐	☐	☐			☐		☐	☐			☐			☐
H2H	8/15	☐				☐	☐	☐	☐			☐	☐			☐
Xi et al.	10/15	☐	☐	☐	☐	☐	☐		☐				☐	☐	☐	
Secret from Muscle	9/15	☐	☐	☐	☐	☐	☐		☐				☐	☐		
Voltkey	8/15	☐	☐	☐	☐			☐		☐			☐			☐

ZIA schemes has a randomness issue

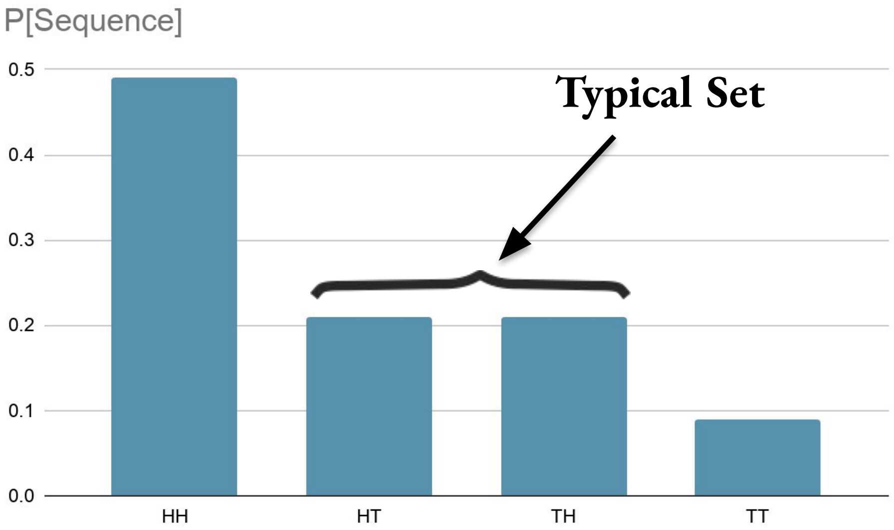
Goal

Improve randomness for low entropy sources → Leads to → Better keys

Requirements

Uniformity	: Evenly distributed key generation
Scalability	: A small bit stream is as random as a long bit stream.
Consistency	: The first bit stream is as random as the last.

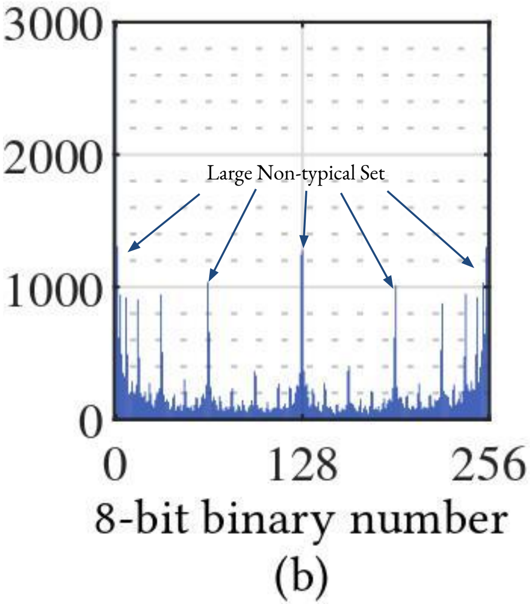
ASYMPTOTIC EQUIPARTITION PROPERTY



- Unfair coin: 70% chance of landing Heads.
- But the sequences HT and TH are equally likely.
- Moonshine extracts the typical set dynamically during runtime.
- Moonshine also discards bits to offset low entropy data skews.

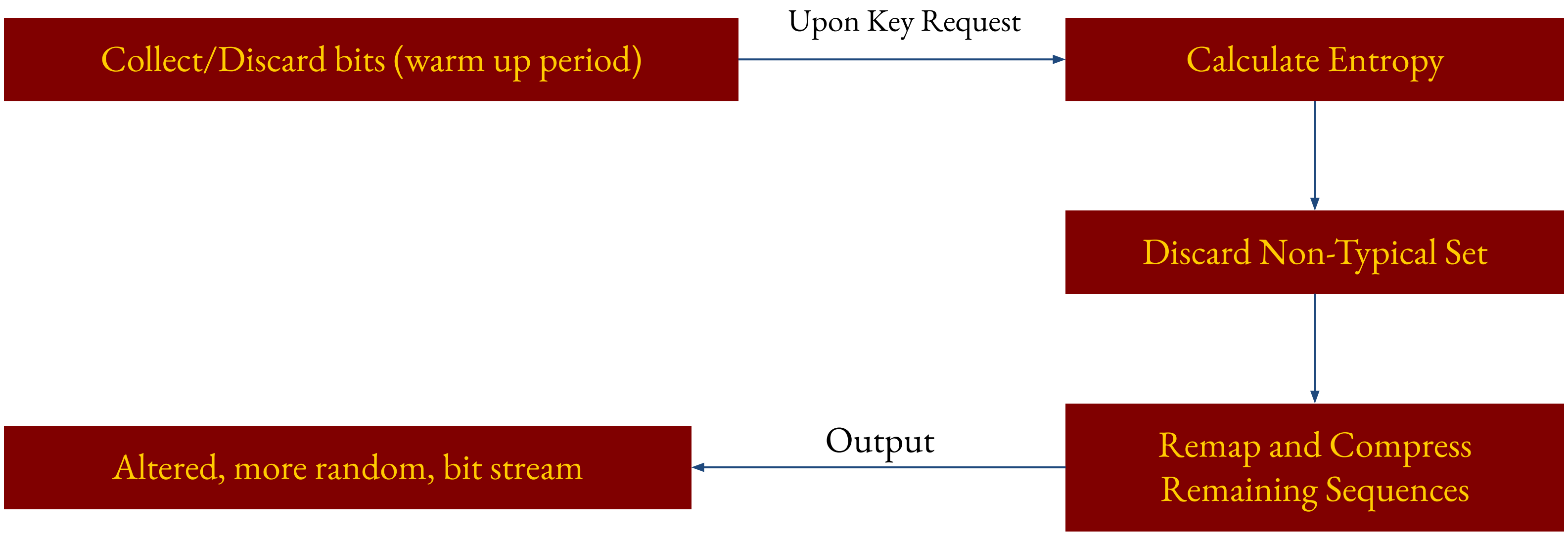
Moonshine and the AEP

Before Moonshine



Moonshine makes Voltkey's data more uniform!

Moonshine



Collect/Discard bits (warm up period)
Upon Key Request
Calculate Entropy
Discard Non-Typical Set
Remap and Compress Remaining Sequences
Output
Altered, more random, bit stream

Sequence length = 4
Discard = 4

Parse Bit Stream

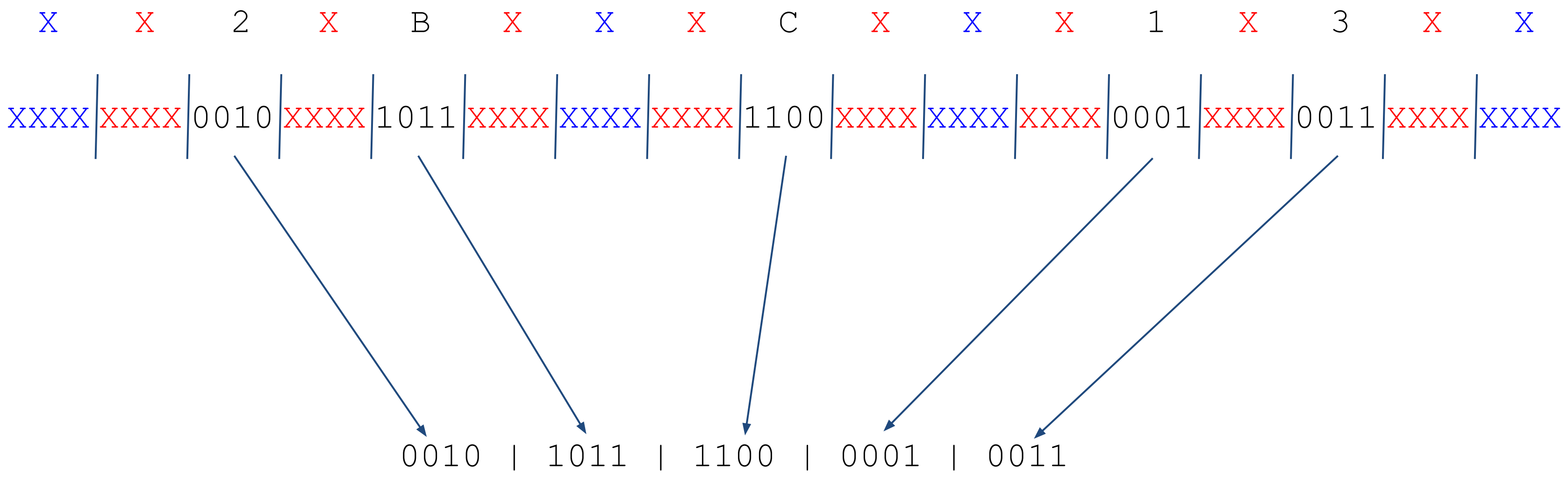
0	1	2	E	B	F	E	A	C	E	0	A	1	0	3	F	E
0000	0001	0010	1110	1011	1111	1110	1010	1100	1110	0000	1010	0001	0000	0011	1111	1110

Discard Bits

0	X	2	X	B	X	E	X	C	X	0	X	1	X	3	X	E
0000	XXXX	0010	XXXX	1011	XXXX	1110	XXXX	1100	XXXX	0000	XXXX	0001	XXXX	0011	XXXX	1110

Manages and monitors the low entropy input

Discard Non-typical Set



Application of AEP

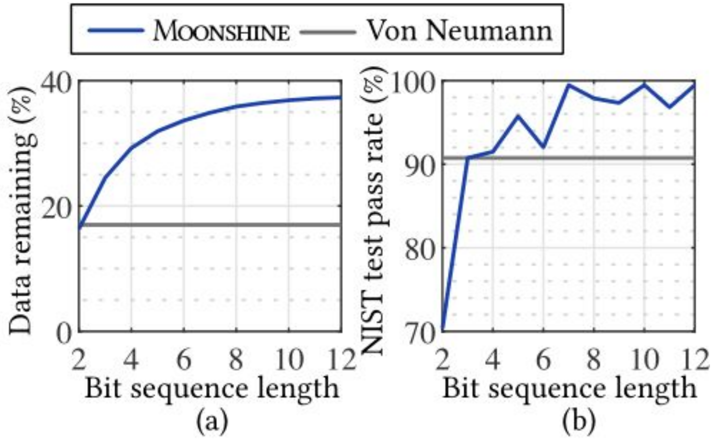
Remap Remaining Bits

0010 | 1011 | 1100 | 0001 | 0011

011 | 001 | 110 | 000 | 101

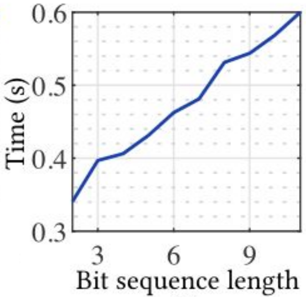
Increases Security

Moonshine Compared directly with Von Neumann's randomness corrector



Moonshine Retains more data and passes more tests than Von Neumann!

Moonshine's Speed. Run on a Voltkey



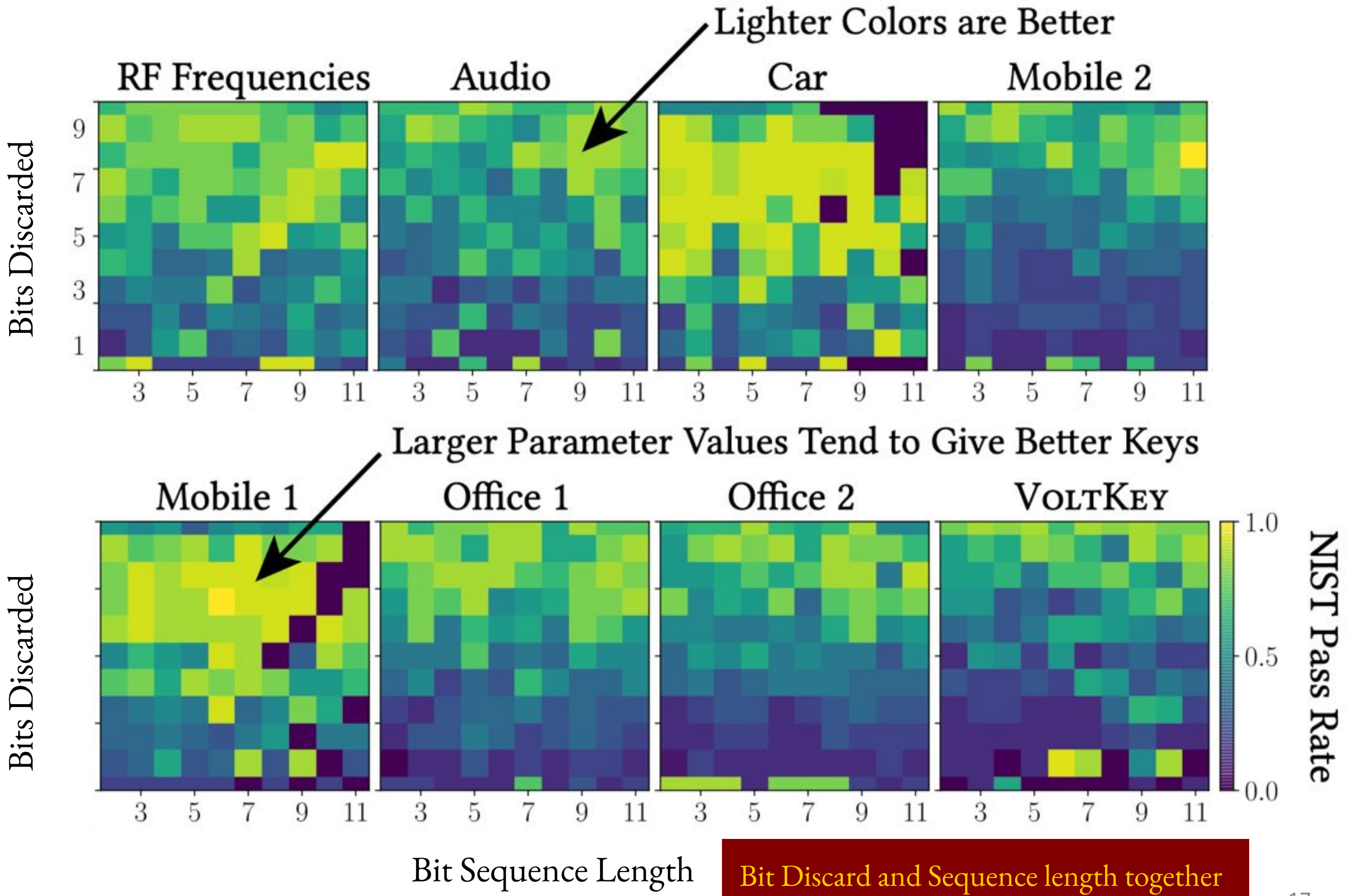
Moonshine's parameters have a linear time complexity relationship!

Longer sequences produce better keys (as predicted by AEP)

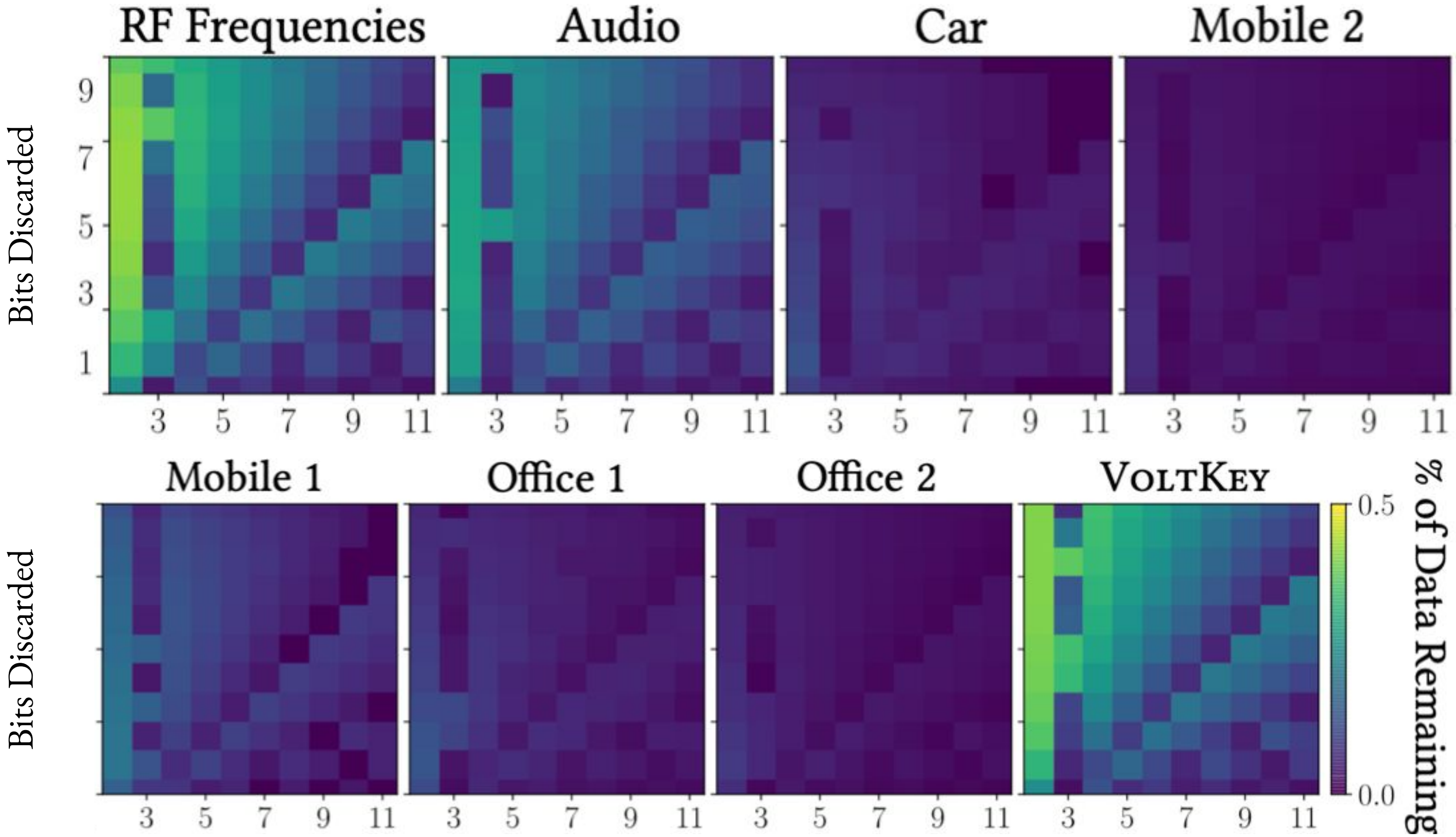
Discard phase breaks up periodicity.

RF Frequencies, Audio, and Voltkey are single entropy sources.

Car, Office and Mobile are a culmination of sources correlated into a bit stream.



Bit Discard and Sequence length together create better randomness!



Voltkey, RF Frequencies, and Audio have initially better entropy.

Bit Sequence Length

Better entropy will allow for Moonshine to keep more data!

General Advice

1. **Filter out as much periodic noise as possible**
2. **Pick a high entropy source**
3. **Use a randomness corrector (Moonshine, Fuzzy Corrector, etc.)**

Conclusions

1. **Further Application of the AEP does lead to better randomness**
2. **Moonshine offers a configurable randomness distiller for any noise source**
3. **ZIA schemes do improve when using Moonshine.**

IPSN 2021

Moonshine: An Online Randomness Distiller for Zero-Involvement Authentication

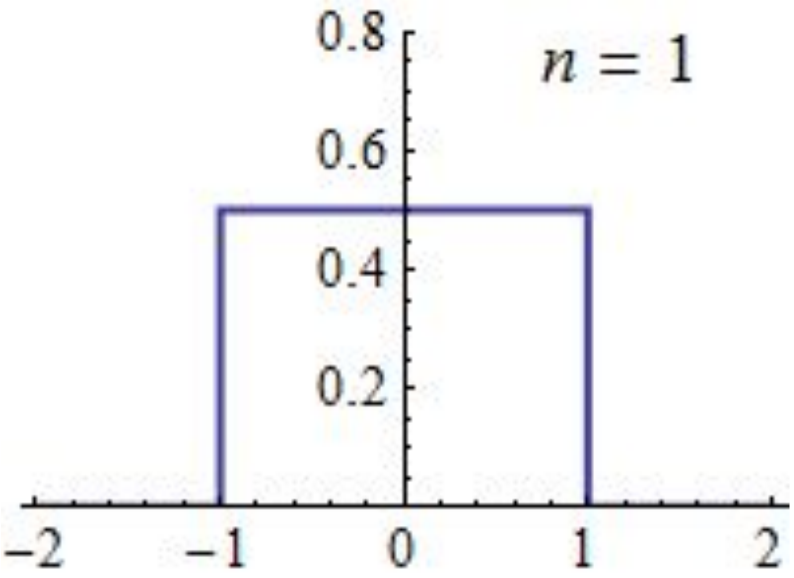
__Jack West__, Kyuin Lee, Suman Banerjee, Younghyun Kim, George K. Thiruvathukal, Neil Klingensmith

jwest1@luc.edu http://jacksonwaynewest.com

LOYOLA UNIVERSITY CHICAGO

WEAK LAW OF LARGE NUMBERS

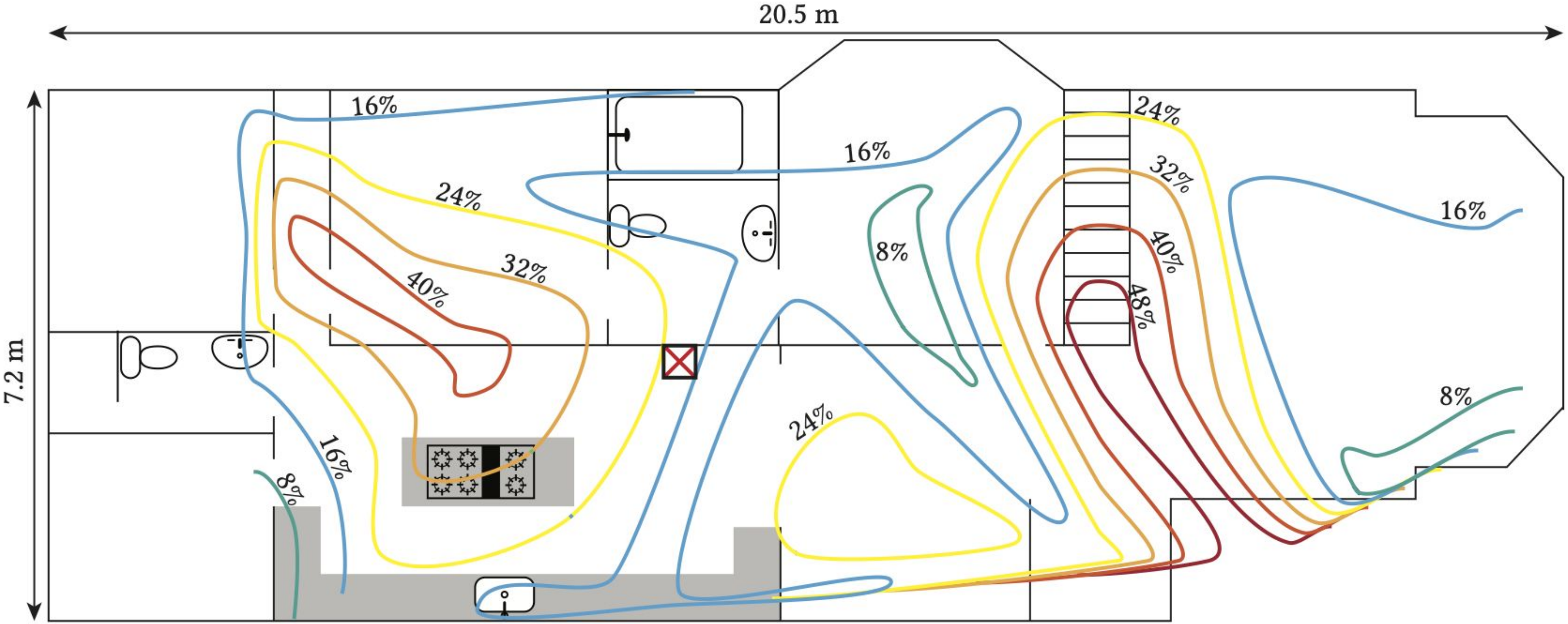
- A sequence of iid samples of a random variable X converges in probability to E[X]



ASYMPTOTIC EQUIPARTITION PROPERTY

- **Weak law's little buddy**
- **Sequences of iid samples of a random variable are approximately uniformly distributed!**
- **No matter the underlying distribution**
- **Uniform approximation gets better as sequences get longer.**

VoltKey



Sequence length = 4
Discard = 4

Parse Bit Stream

0	1	0	0	3	6	7	6	2	5	7	7	6	2	1	1	7	6	1	7	4	3	2
000	001	000	000	011	110	111	110	010	101	111	111	110	010	001	001	111	110	001	111	100	011	010

Discard Bits

0	X	0	X	3	X	7	X	2	X	7	X	6	X	1	X	7	X	1	X	4	X	2
000	XXX	000	XXX	011	XXX	111	XXX	010	XXX	111	XXX	110	XXX	001	XXX	111	XXX	001	XXX	100	XXX	010

Sequence length = 4
Discard = 4

Parse Bit Stream

0 1 2 E B F E A C E 0 A 1 0 3 F E

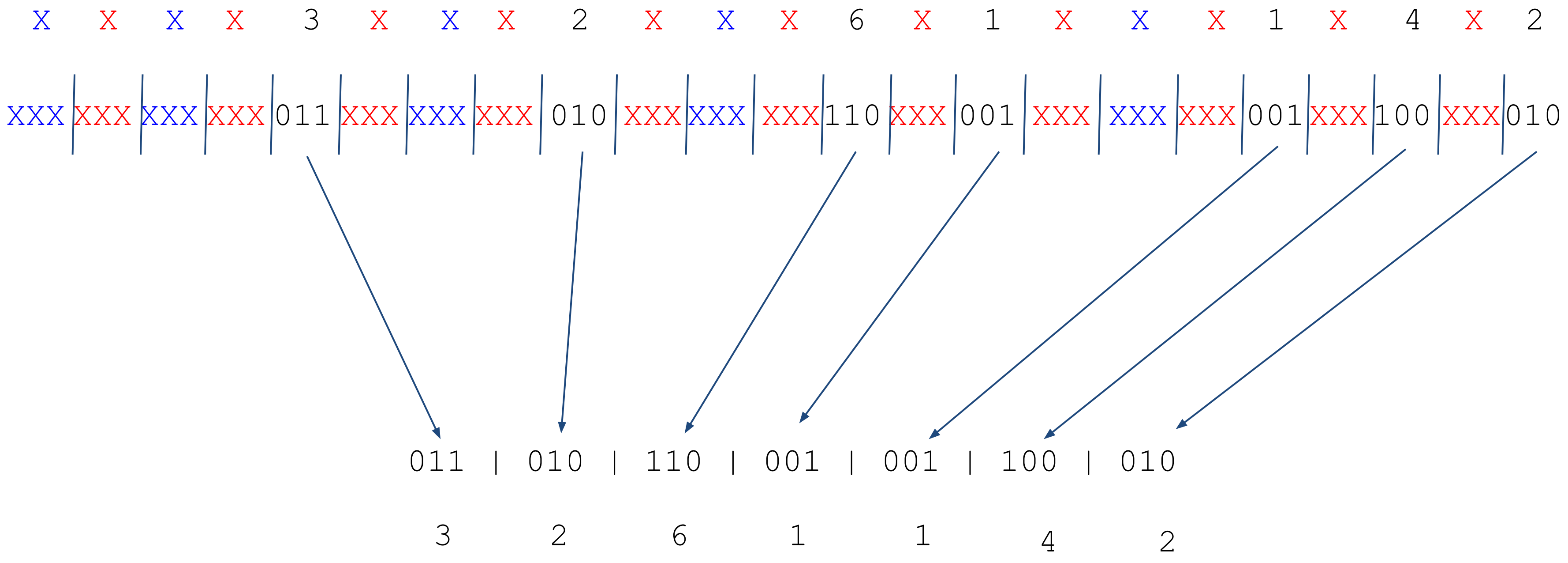
0000 | 0001 | 0010 | 1110 | 1011 | 1111 | 1110 | 1010 | 1100 | 1110 | 0000 | 1010 | 0001 | 0000 | 0011 | 1111 | 1110

Discard Bits

0 X 2 X B X E X C X 0 X 1 X 3 X E

0000 | XXXX | 0010 | XXXX | 1011 | XXXX | 1110 | XXXX | 1100 | XXXX | 0000 | XXXX | 0001 | XXXX | 0011 | XXXX | 1110

Discard Non-typical Set

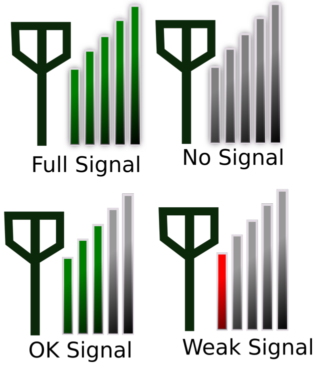


ECG (Heart2Heart)

Ambient Audio (DEMAND)

RF Signals (ProxiMate)

RSS (Ensamble)



Remap Remaining Bits

0010 | 1011 | 1100 | 0001 | 0011

011 | 001 | 110 | 000 | 101

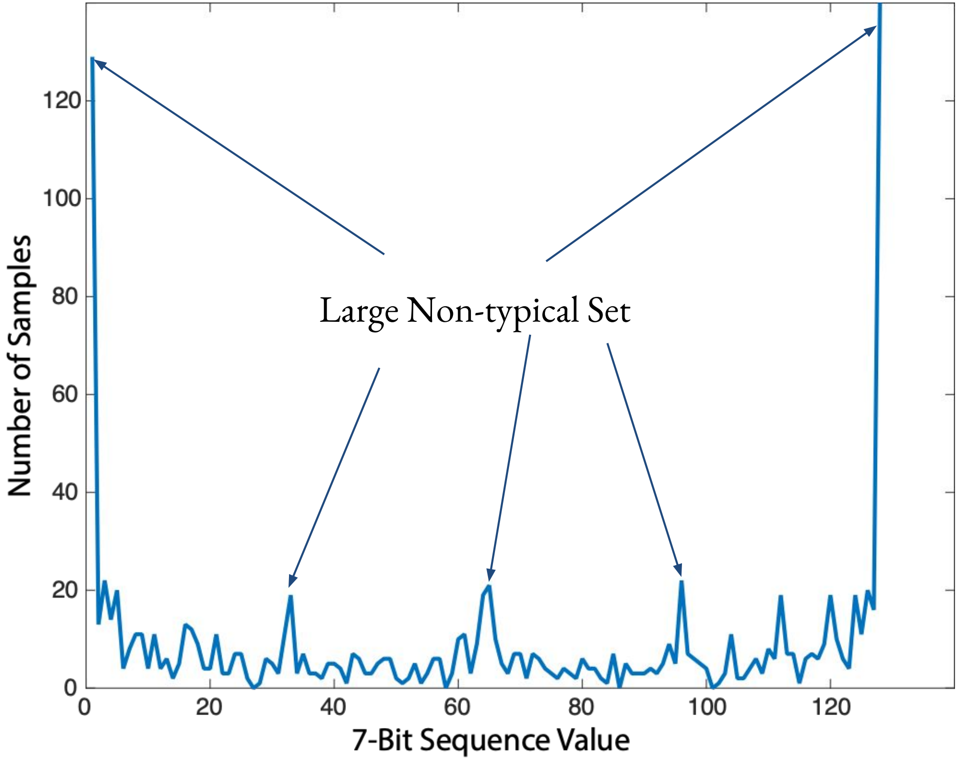
NIST Randomness Evaluation Suite

Focuses of the NIST tests:

- **Uniformity**
- **Scalability**
- **Consistency**

ASYMPTOTIC EQUIPARTITION PROPERTY

Bit sequences gathered from Voltkey at runtime.



Voltkey's large non-typical set leads to worse randomness

Slide 4 papers

- https://www.researchgate.net/publication/330988253_Biometric-based_Authentication_Scheme_for_Implantable_Medical_Devices_during_Emergency_Situations
- https://www.researchgate.net/publication/221568367_Key_Generation_Based_on_Acceleration_Data_of_Shaking_Processes
- https://homes.cs.washington.edu/~lamarca/pubs/ensemble_mobisys10.pdf
-