Royal Holloway
University of London

On the Security of RC4 in TLS

Nadhem AlFardan, Dan Bernstein, Kenny Paterson, Bertram Poettering, Jacob Schuldt

Royal Holloway, University of London
University of Illinois at Chicago

http://www.isg.rhul.ac.uk/tls/

UIC

TLS Record Protocol

CBC-mode
(AES, 3DES)

RC4

TLS Record Protocol

Information Security Group

CBC-mode
ES, 3DES)

BEAST attack

RC4

TLS Record Protocol

CBC-mode
ES, 3DES,

RC4

BEAST attack

Lucky 13

TLS Record Protocol

CBC-mode
ES, 3DES)

BEAST attack

Lucky 13

RC4

Switch to RC4?

TLS Record Protocol

Information Security Group

CBC-mode
AES, 3DES, ...

BEAST attack

Lucky 13

RC4

Switch to RC4?

Recommended!

Usage of RC4 in Practice

ICSI Certificate Notary

Recent survey of 16 billion TLS connections:
Approx. 50% protected via RC4 ciphersuites

Usage of RC4 in Practice

ICSI Certificate Notary

Recent survey of 16 billion TLS connections:
Approx. 50% protected via RC4 ciphersuites

How secure is TLS + RC4?

RC4 Keystream Distribution

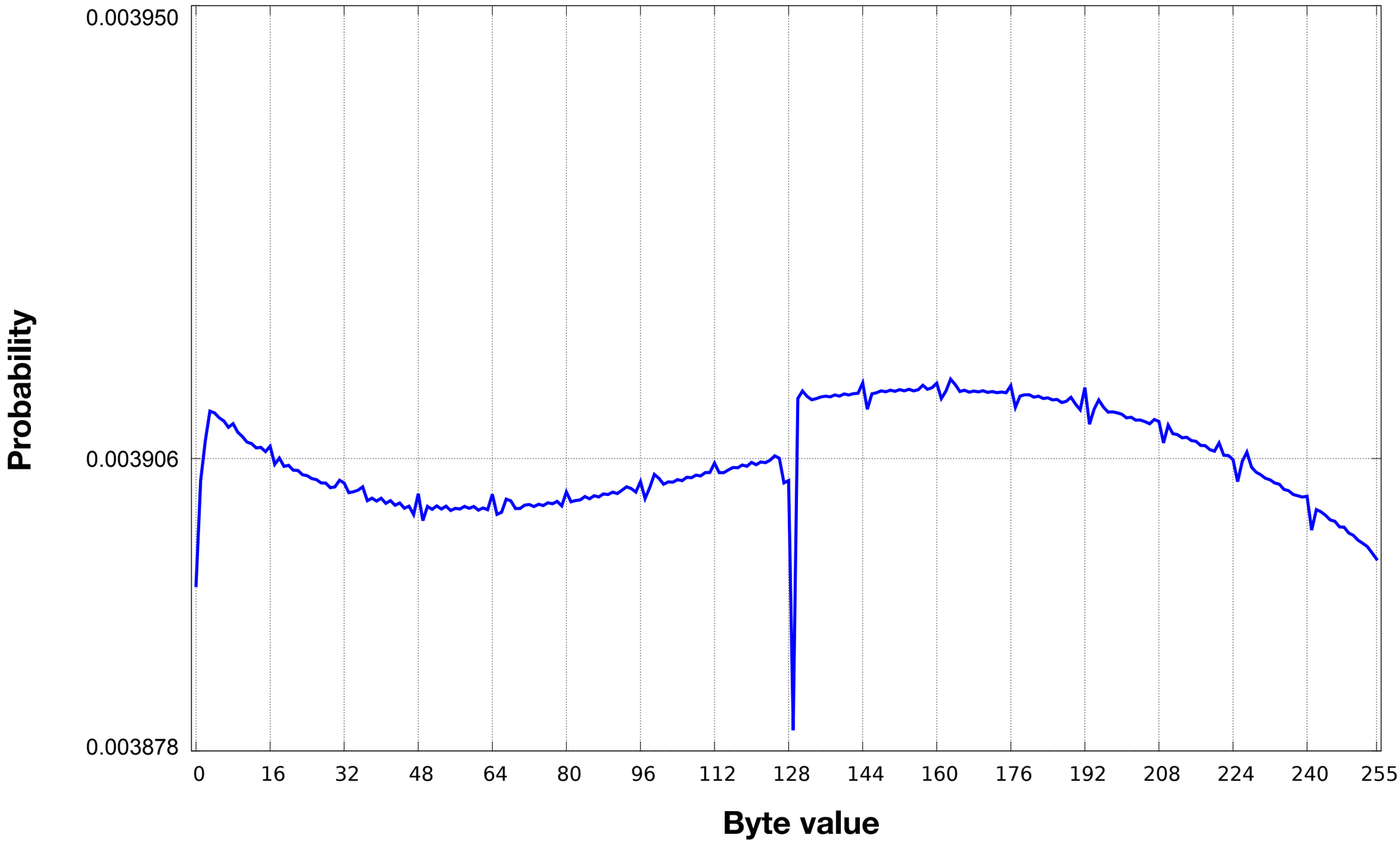
2^{45}

Random RC4 keys

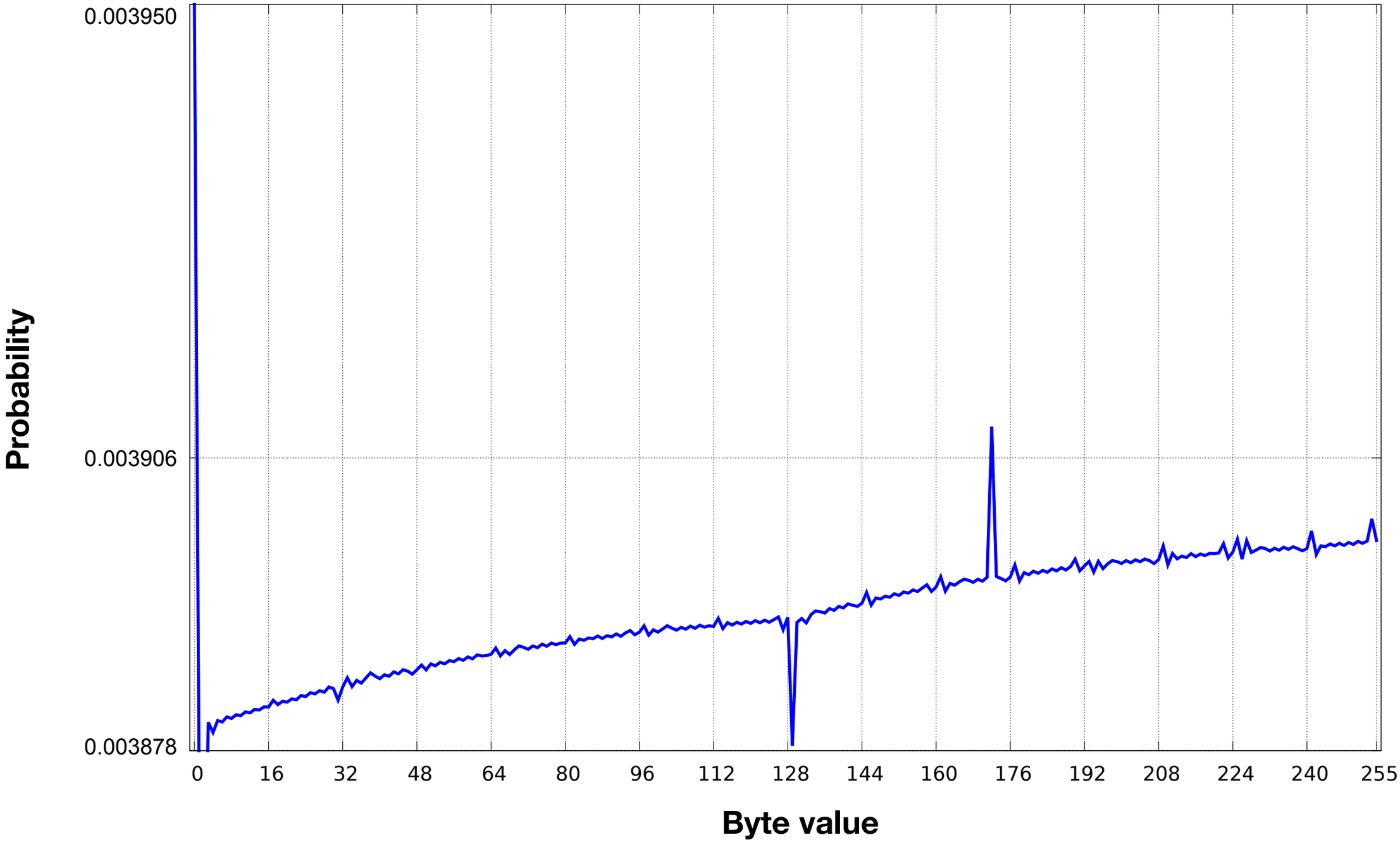
256

Keystream bytes

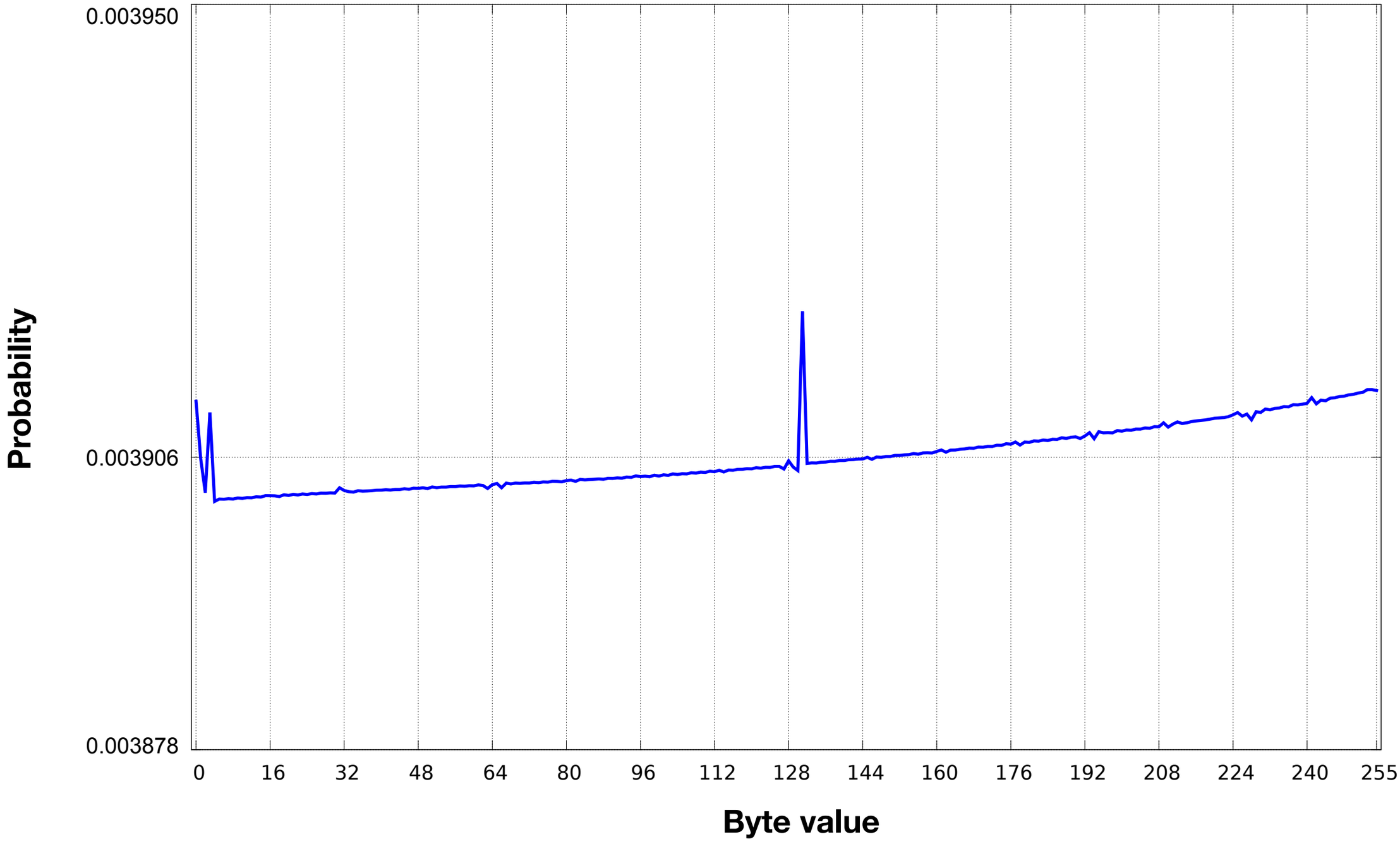
Keystream Distribution at Position 1



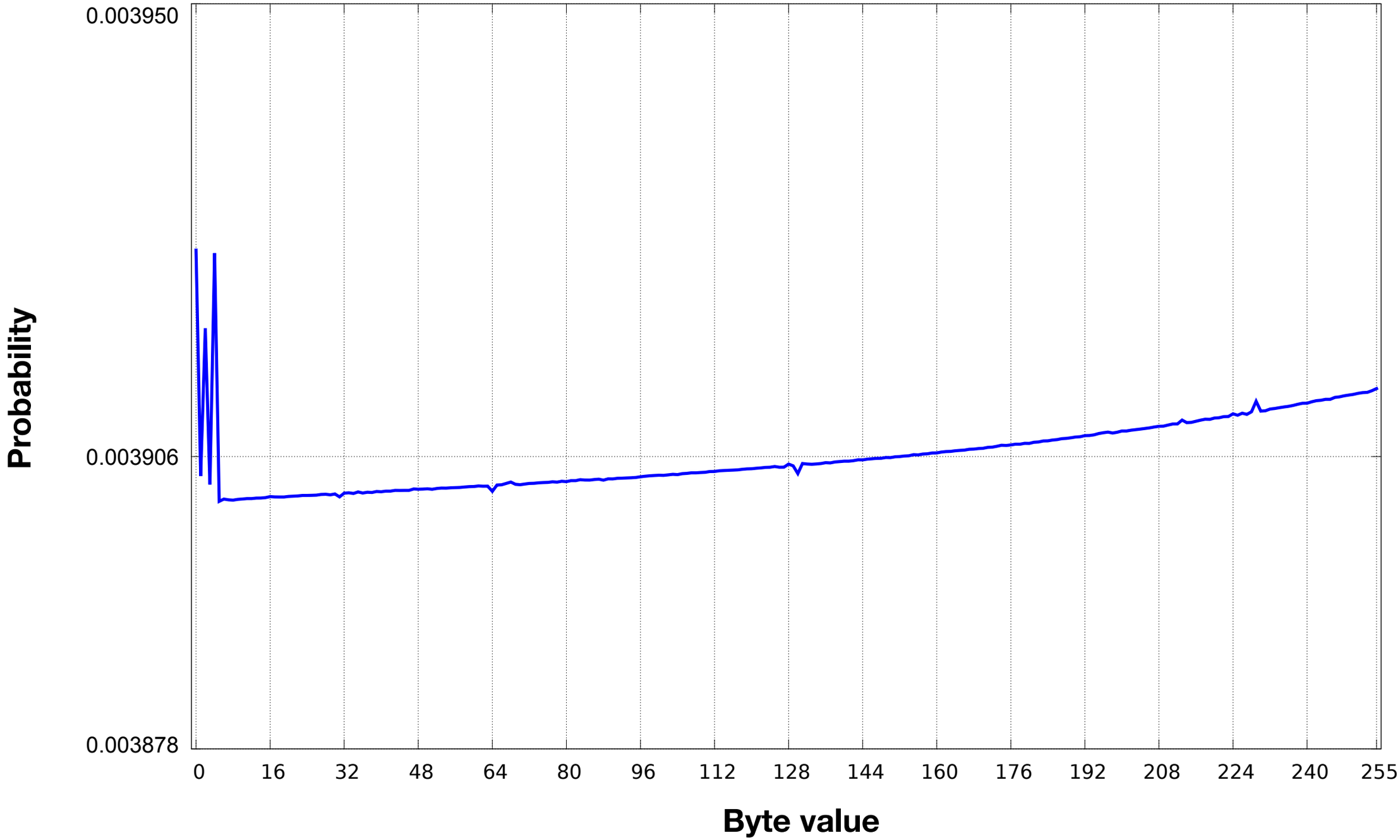
Keystream Distribution at Position 2



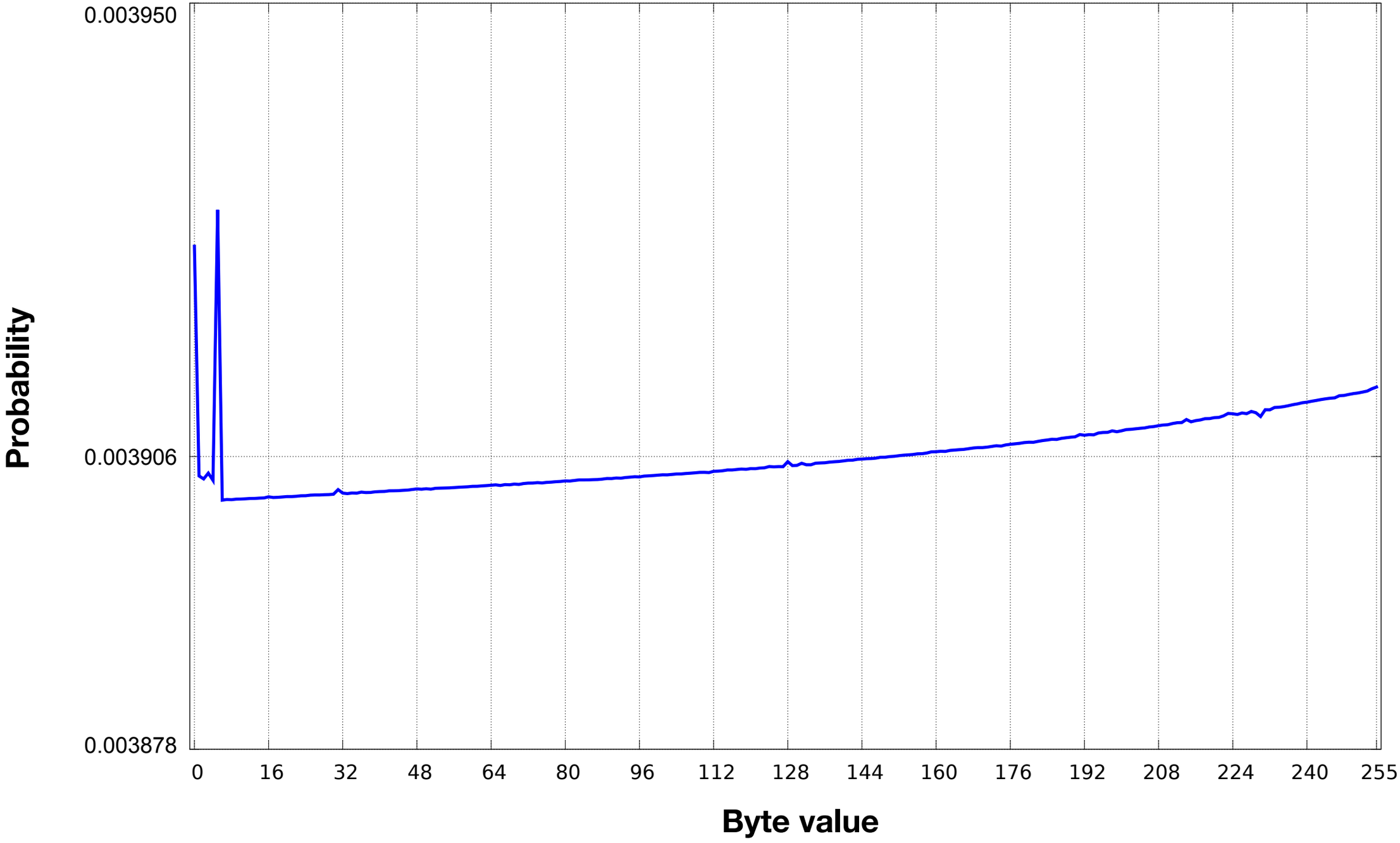
Keystream Distribution at Position 3



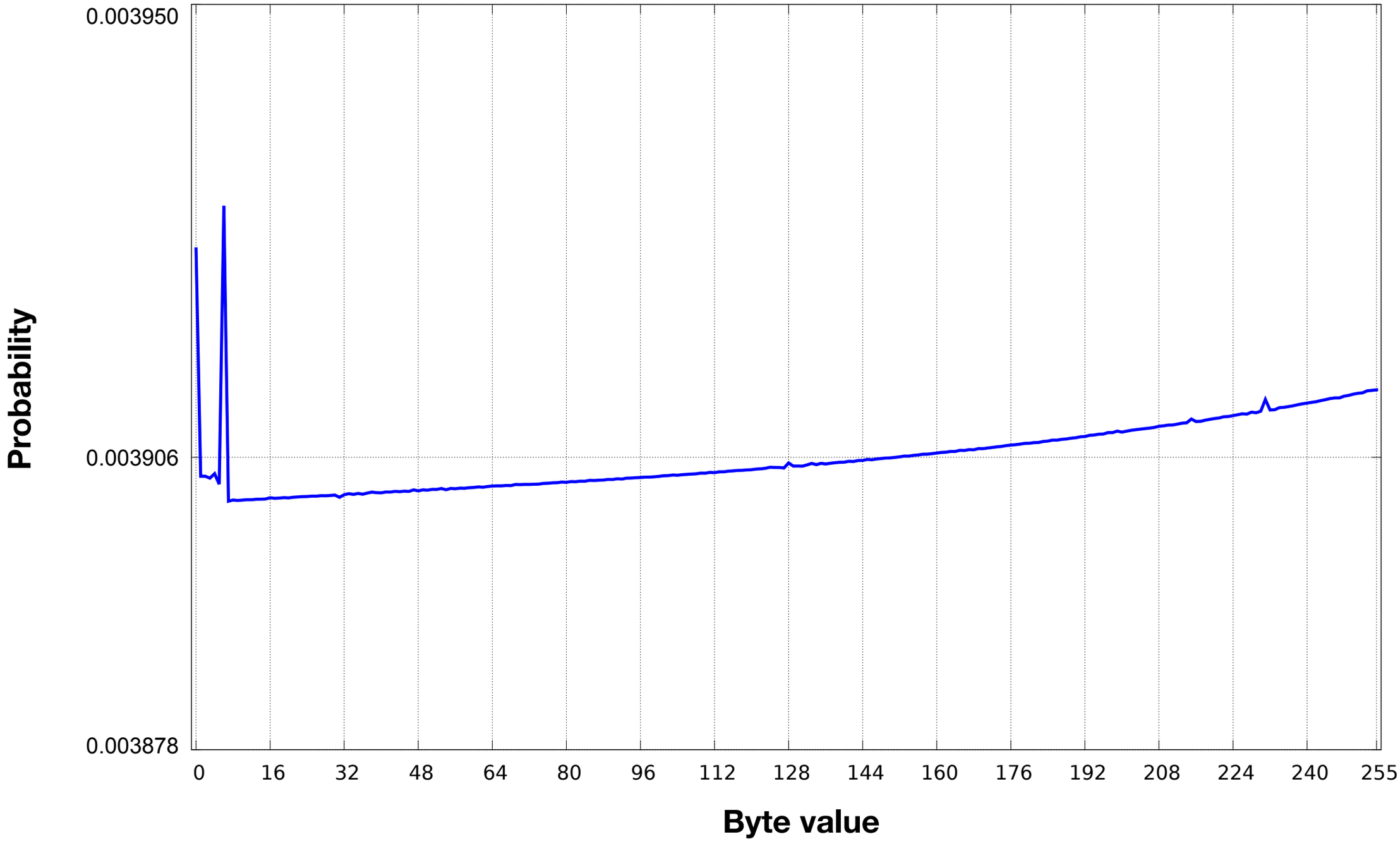
Keystream Distribution at Position 4



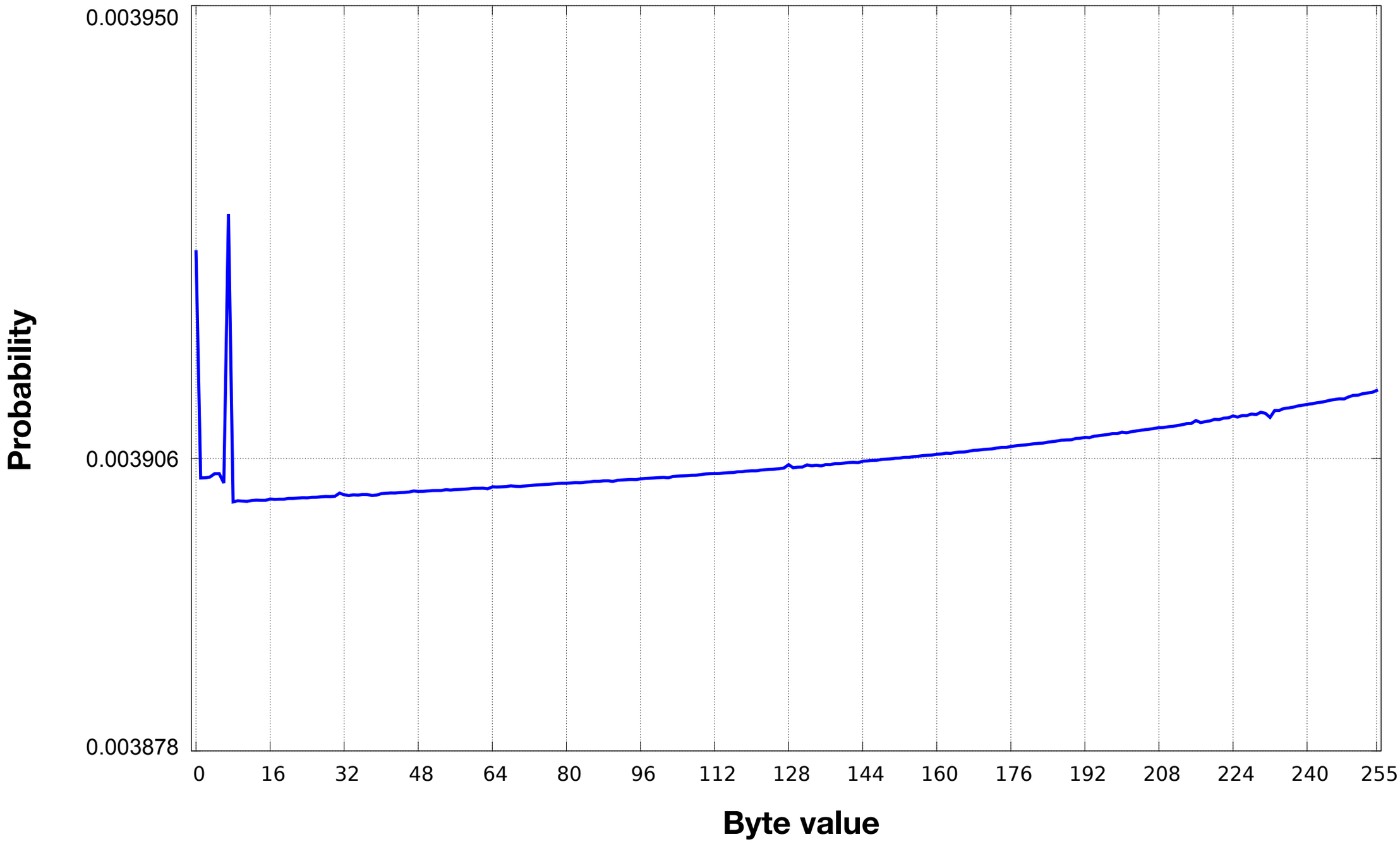
Keystream Distribution at Position 5



Keystream Distribution at Position 6

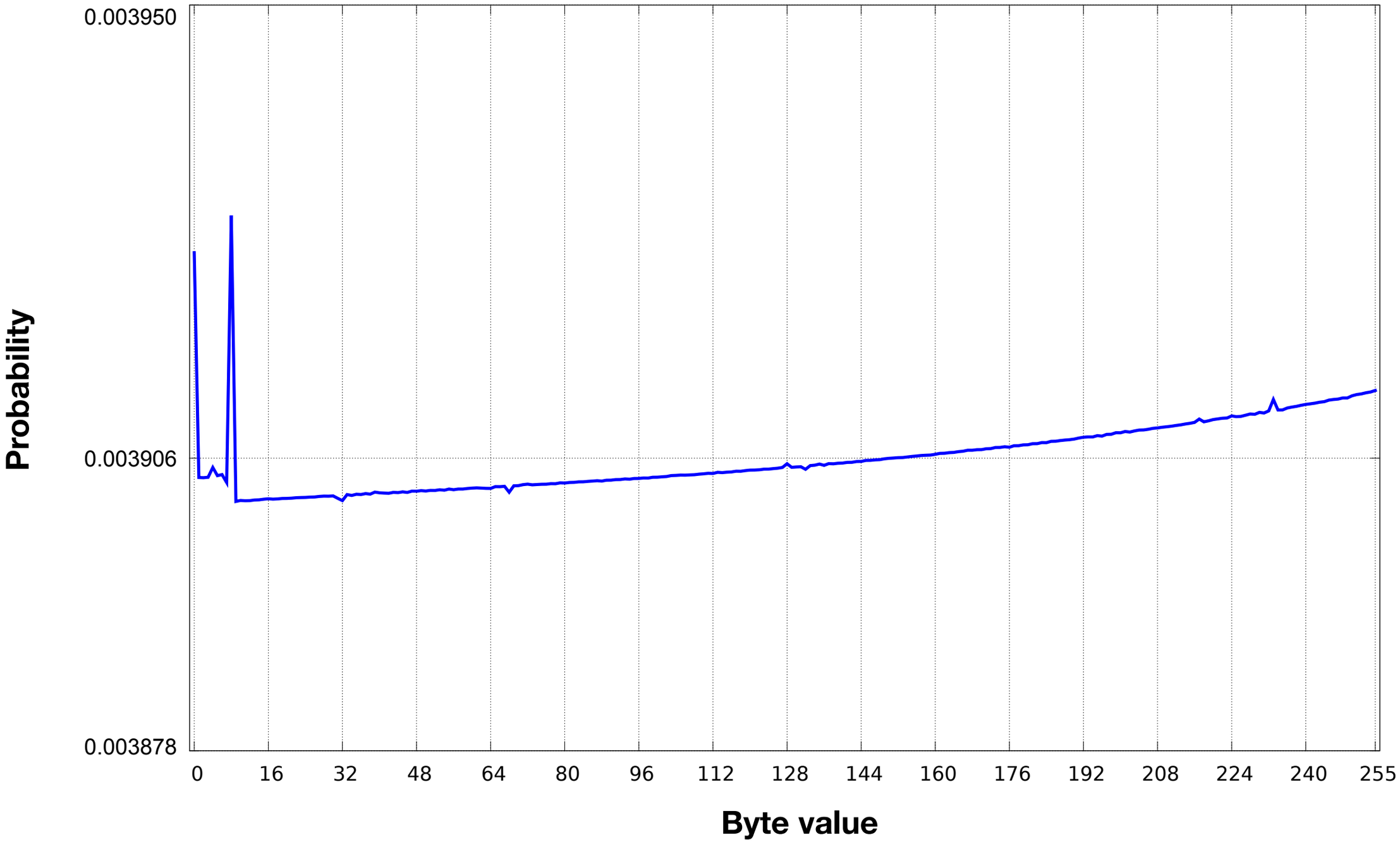


Keystream Distribution at Position 7

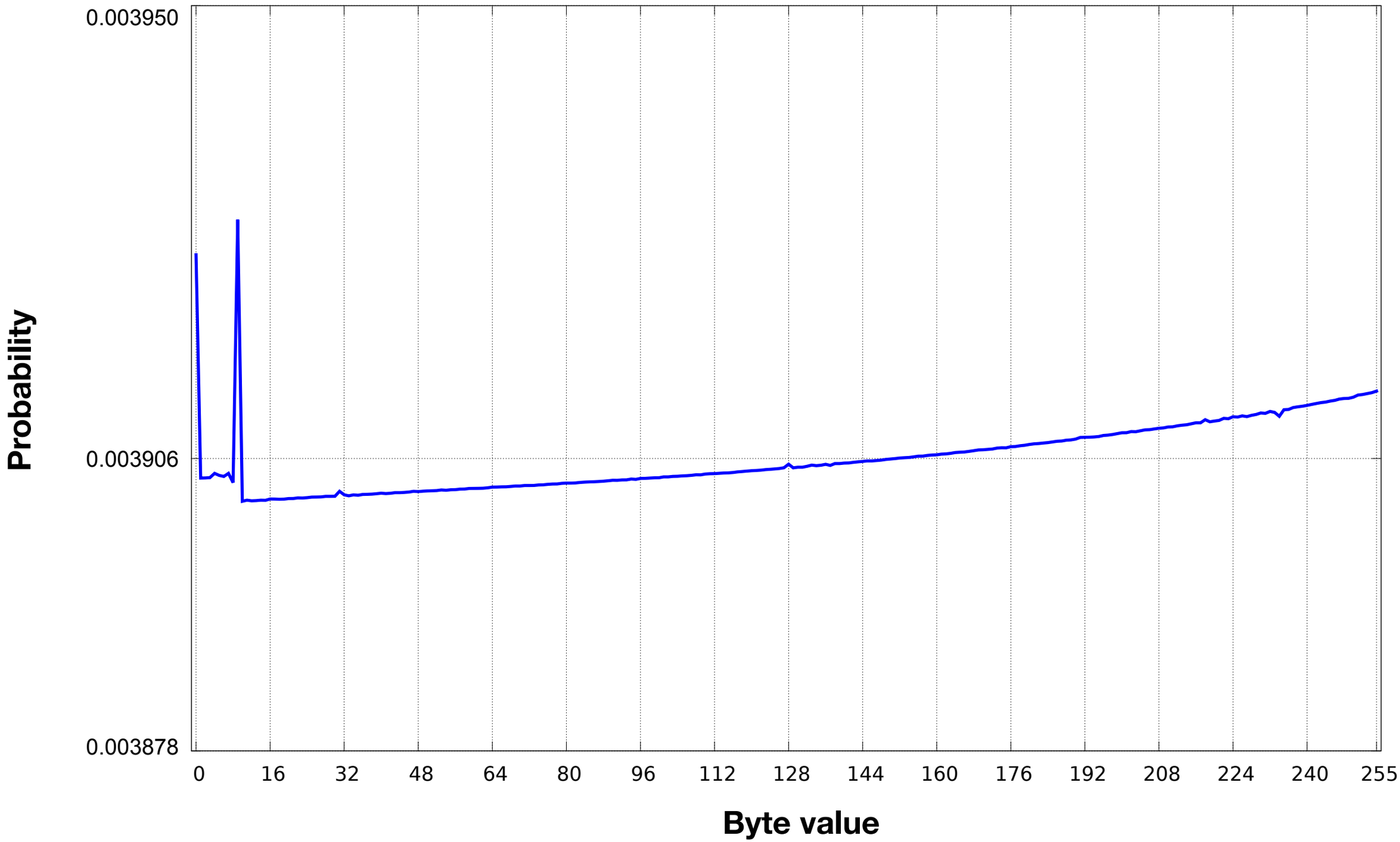


Keystream Distribution at Position 8

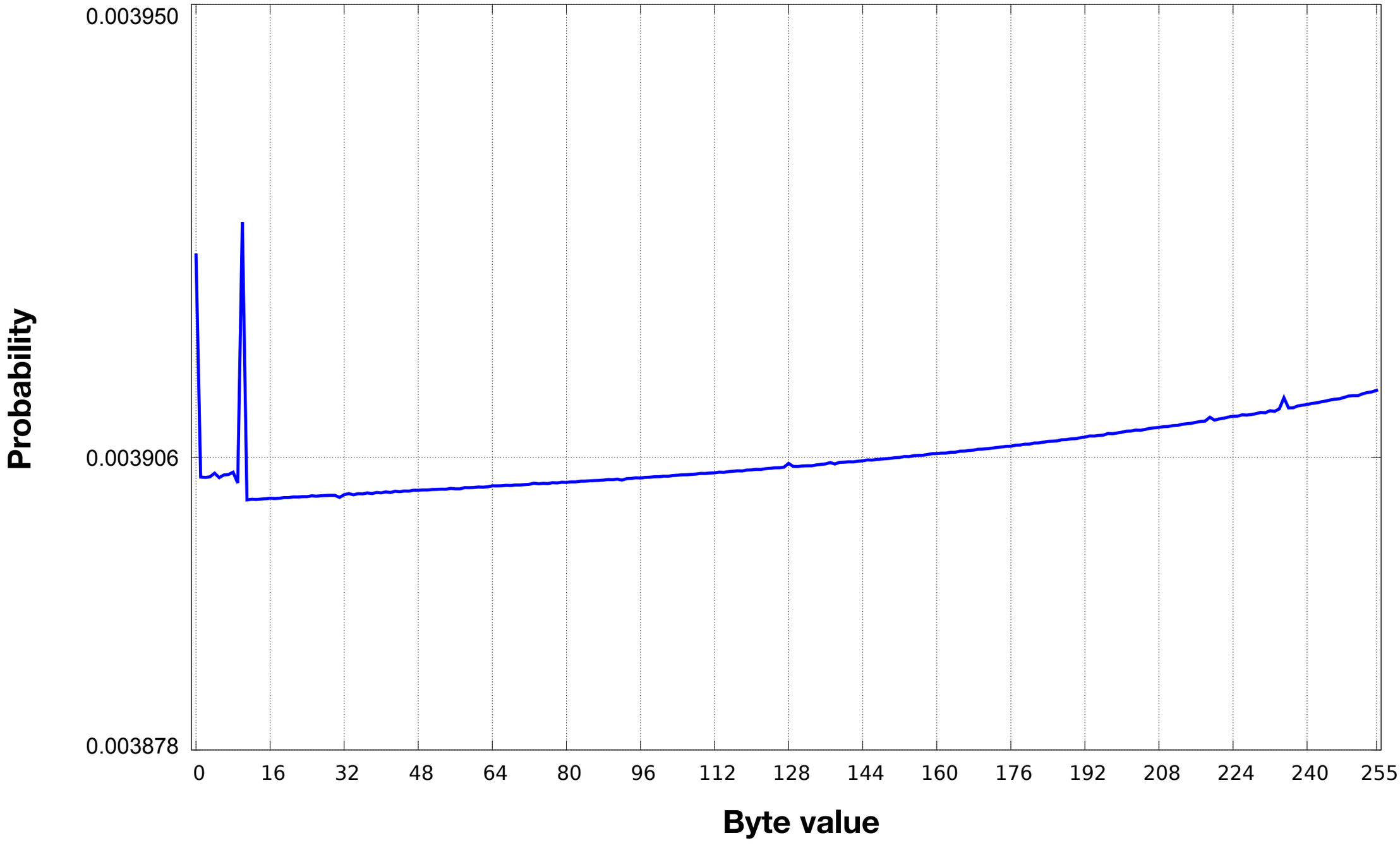
Information Security Group



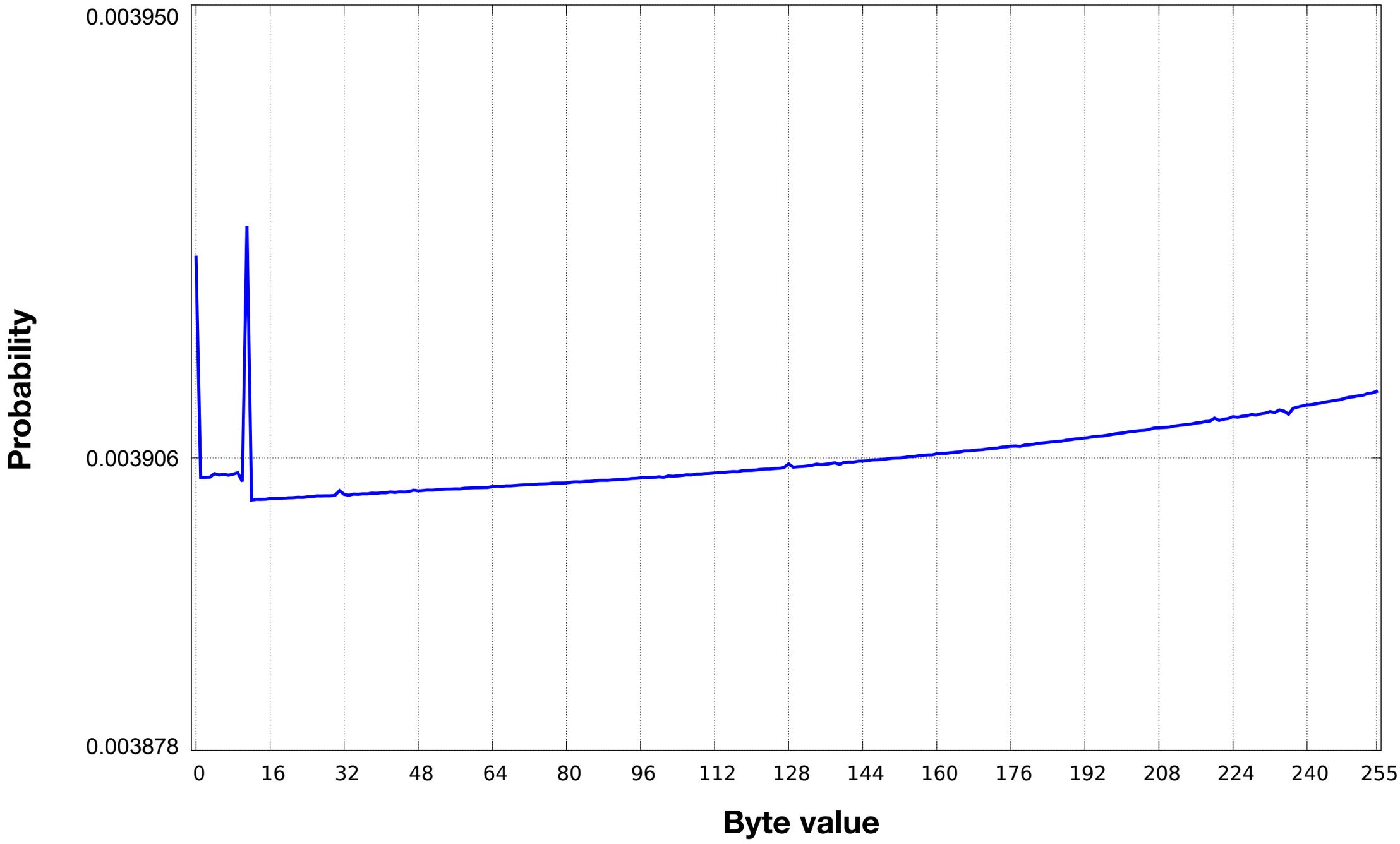
Keystream Distribution at Position 9



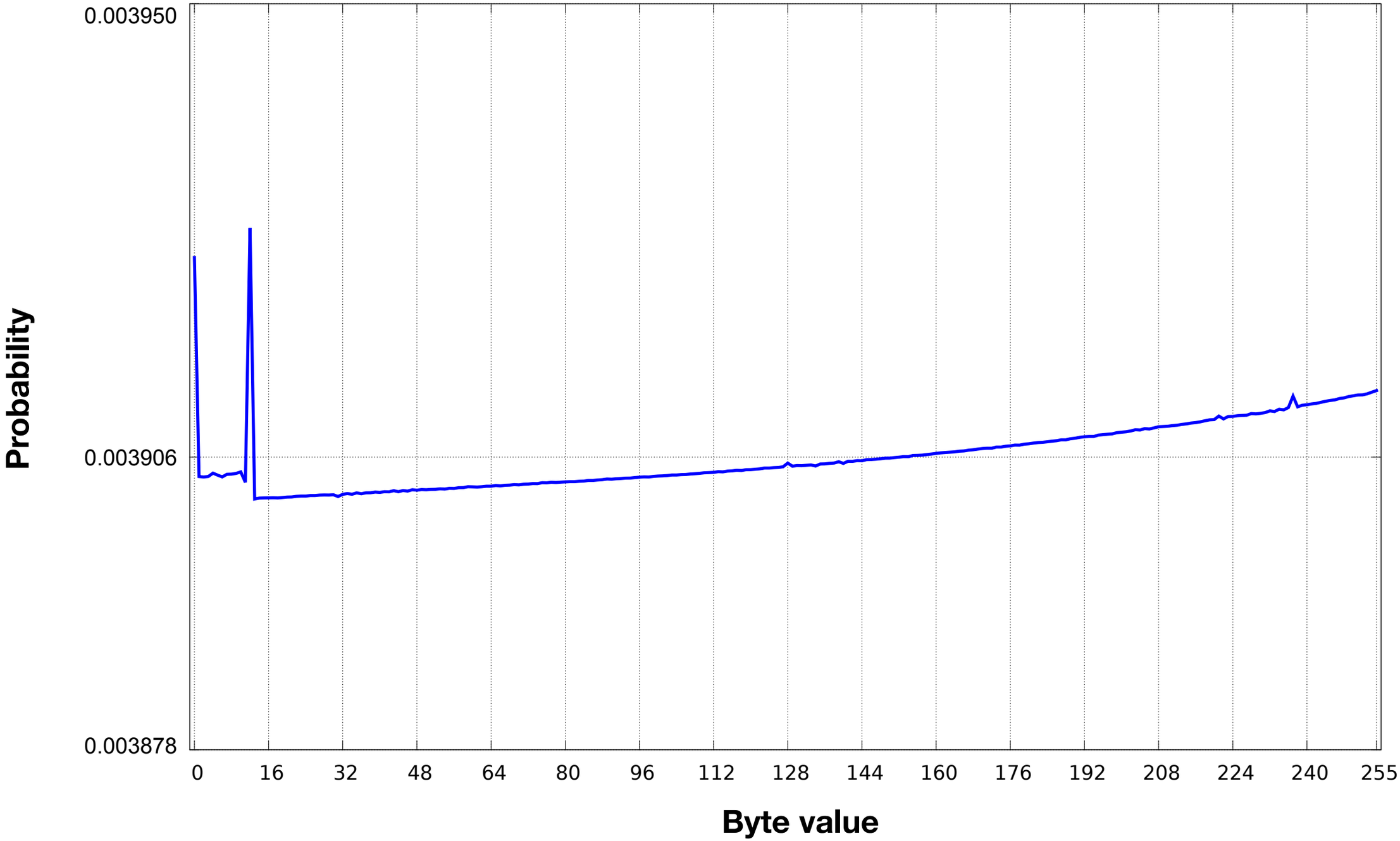
Keystream Distribution at Position 10



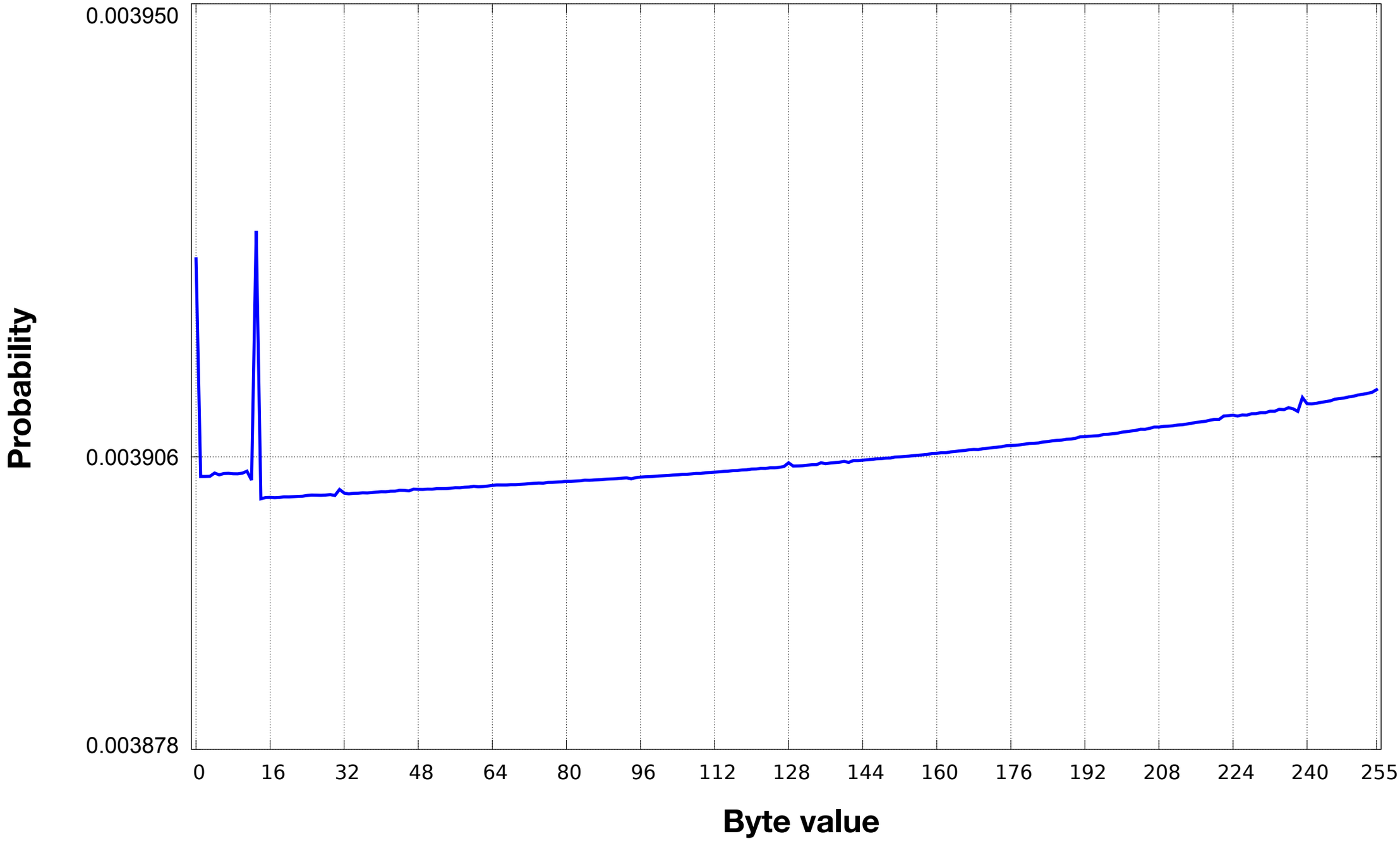
Keystream Distribution at Position 11



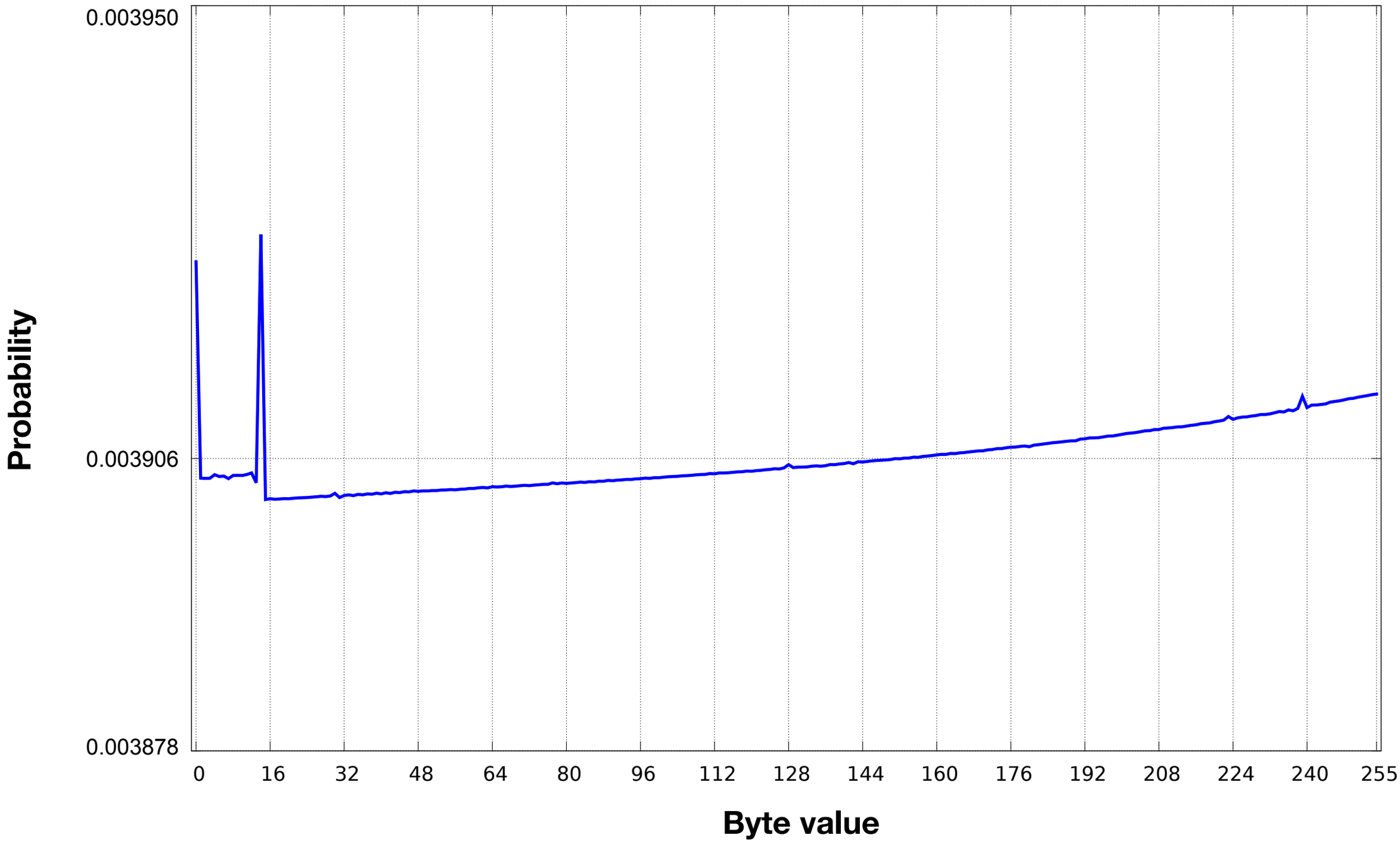
Keystream Distribution at Position 12



Keystream Distribution at Position 13

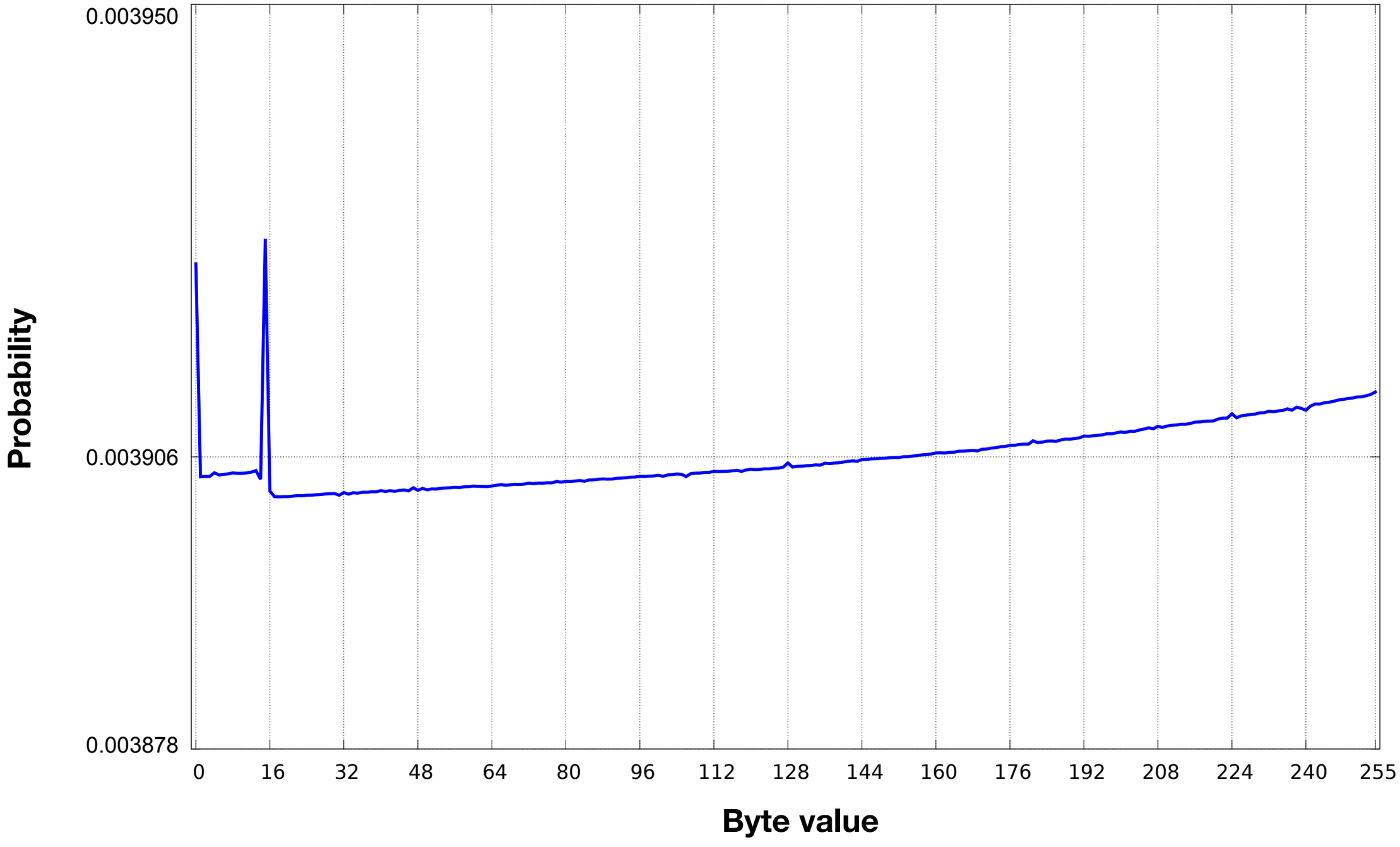


Keystream Distribution at Position 14

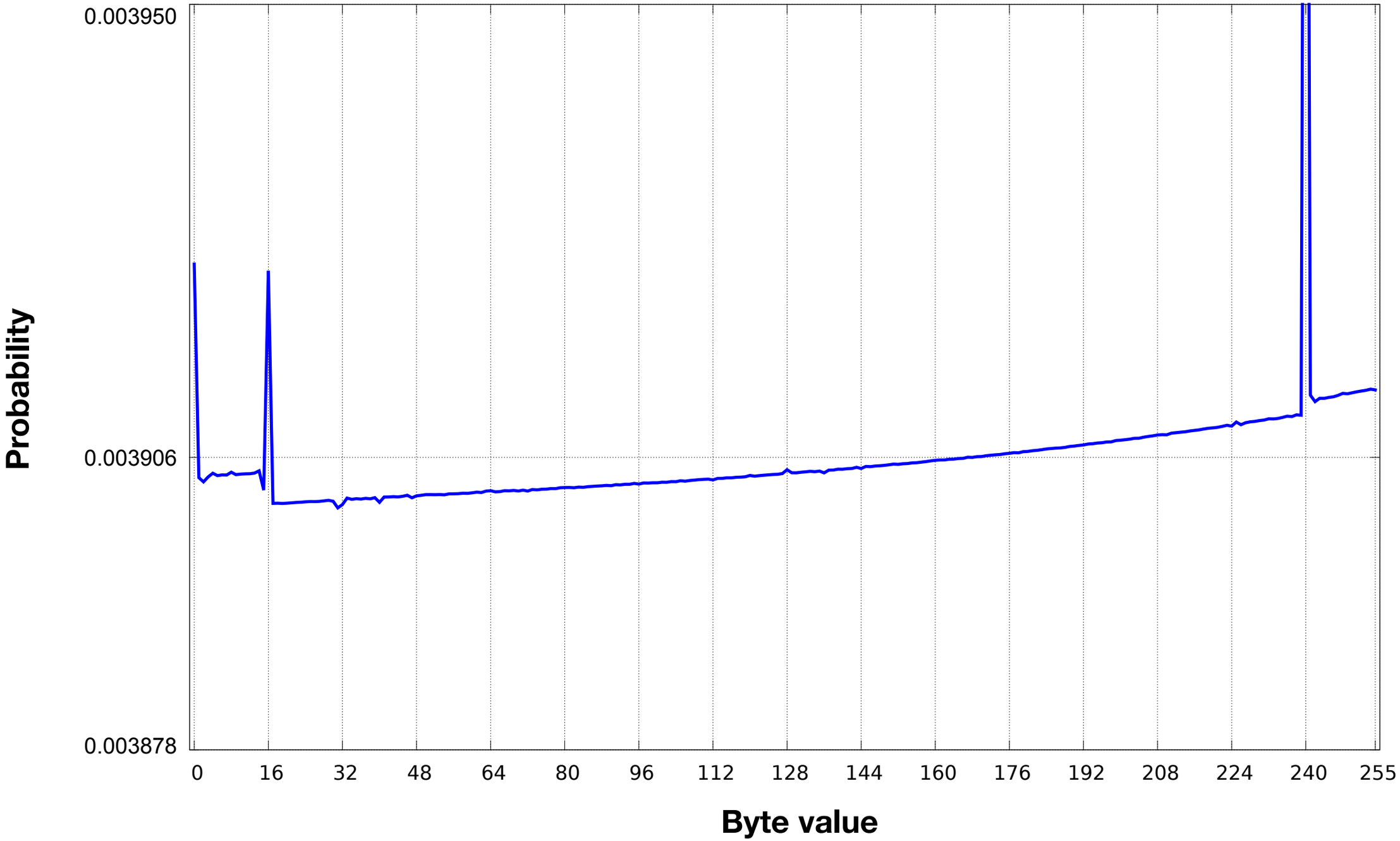


Keystream Distribution at Position 15

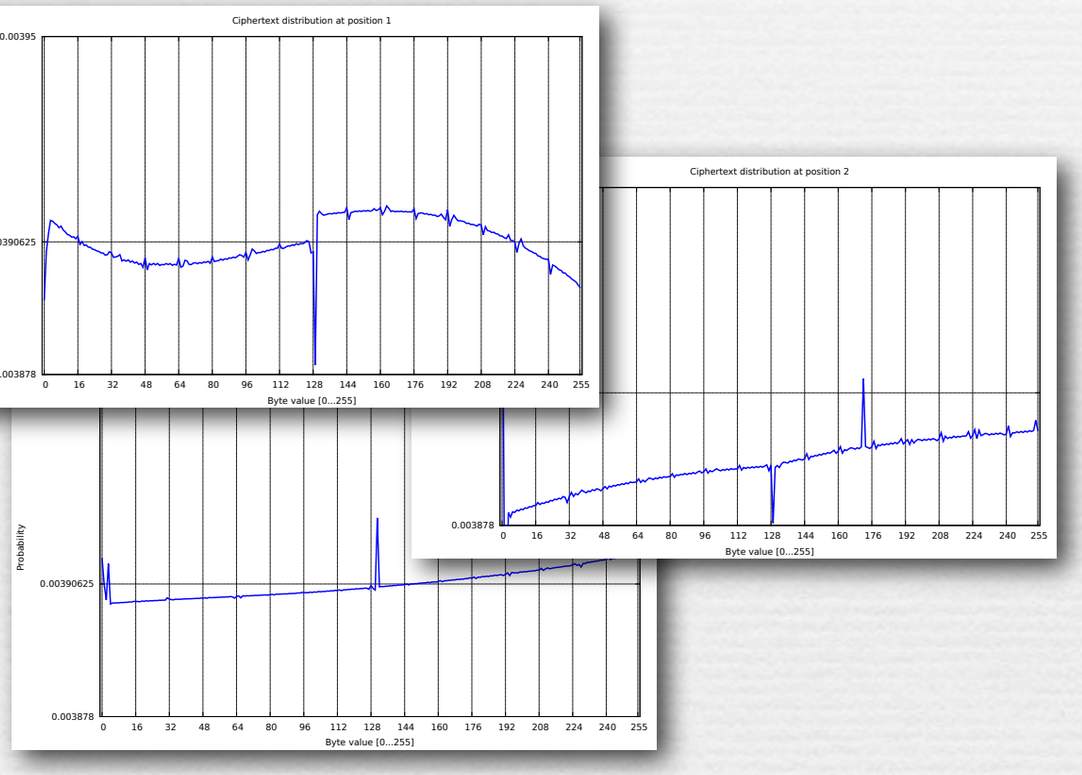
Information Security Group



Keystream Distribution at Position 16



Plaintext Recovery Attack

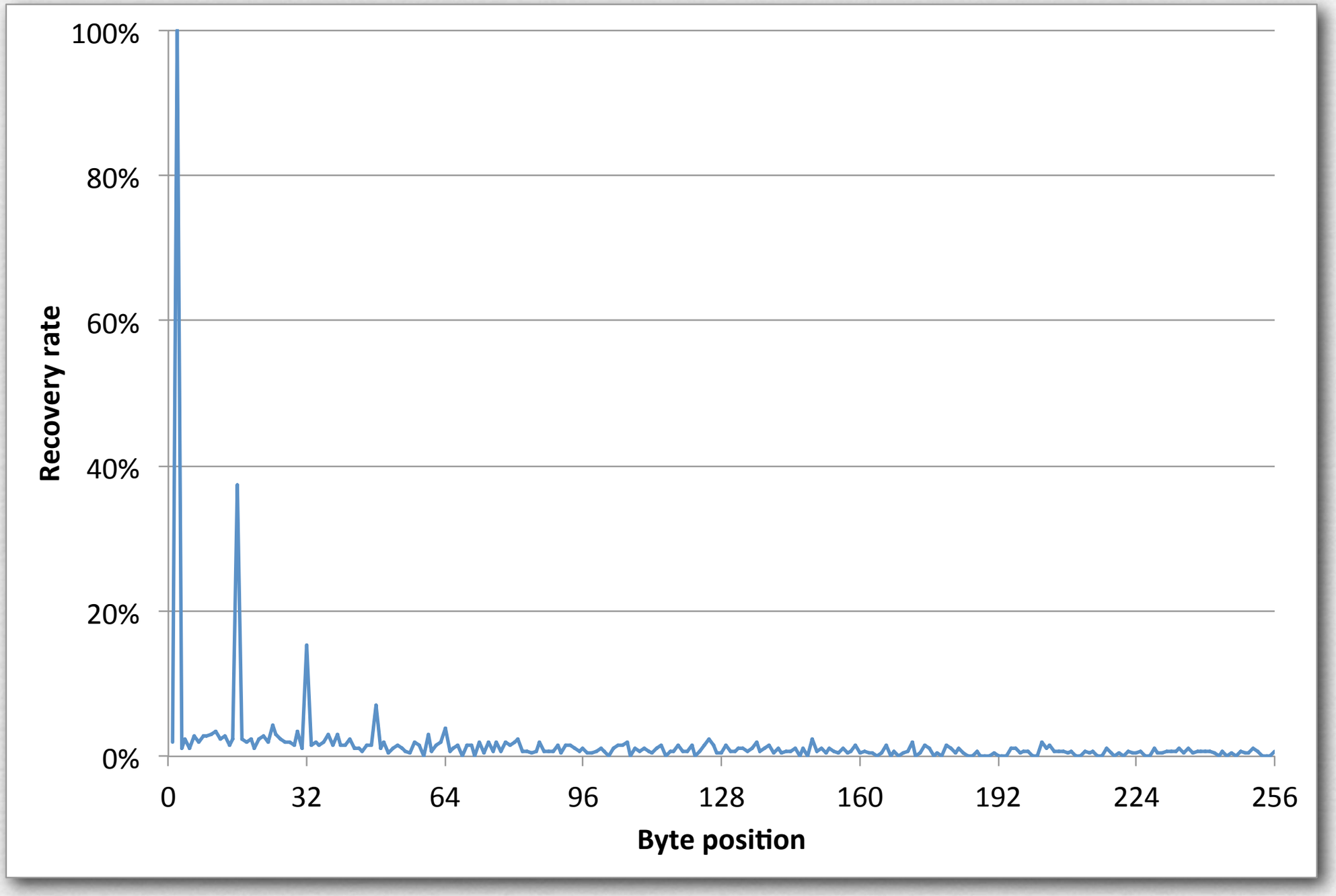


+

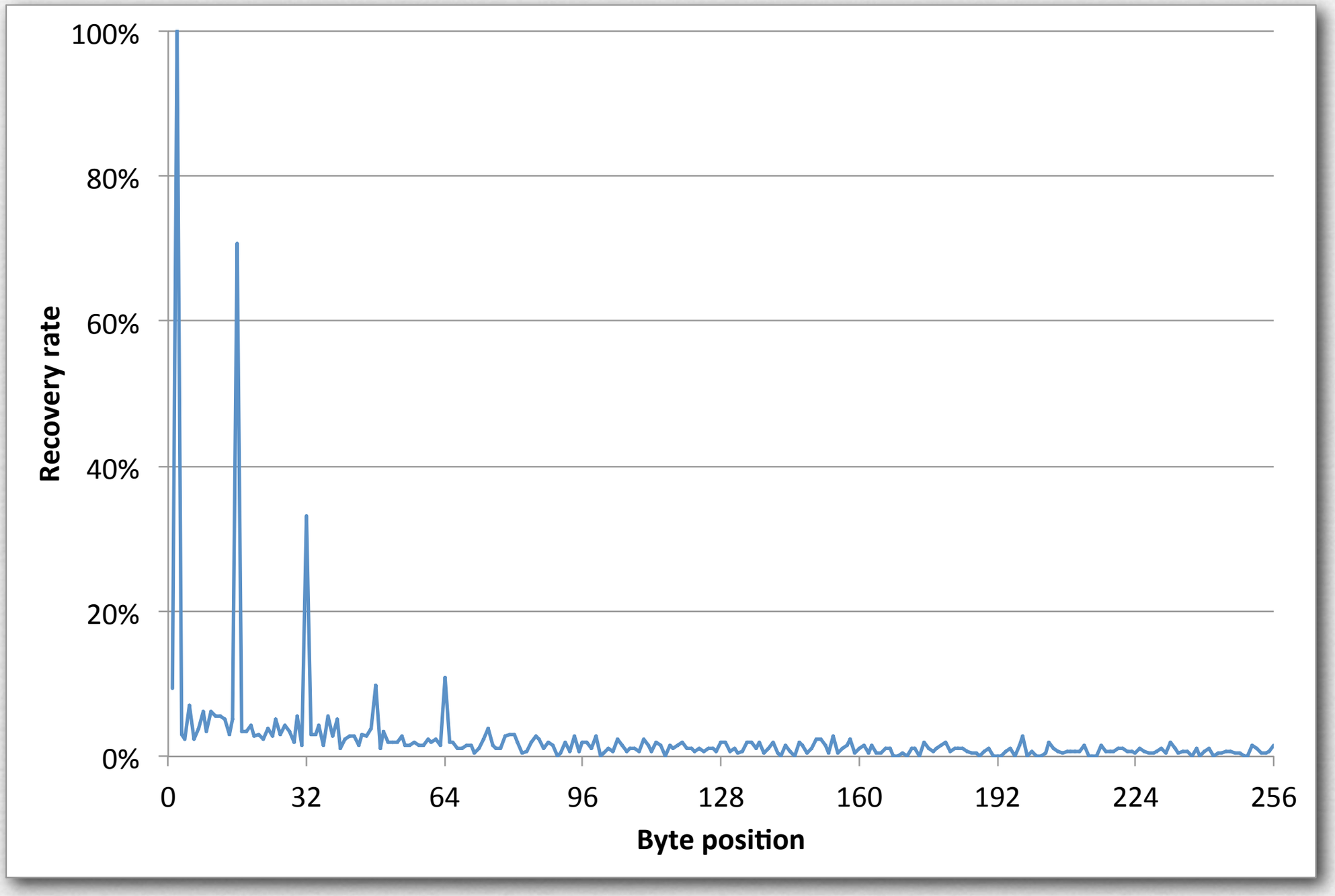
⇓

TLS plaintext recovery
(initial bytes)

Success Probability
2^{20} Sessions

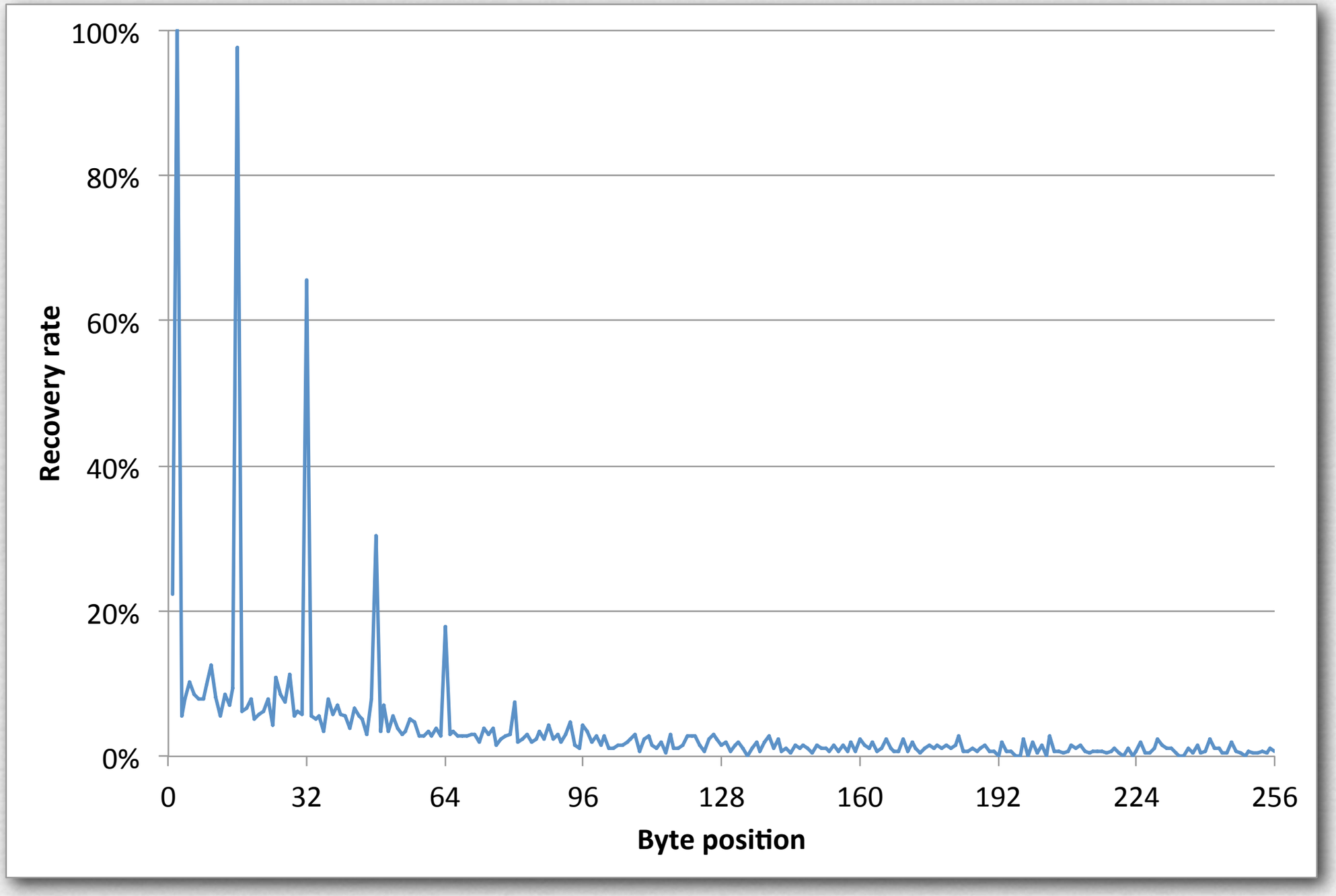


Success Probability
2^{21} Sessions

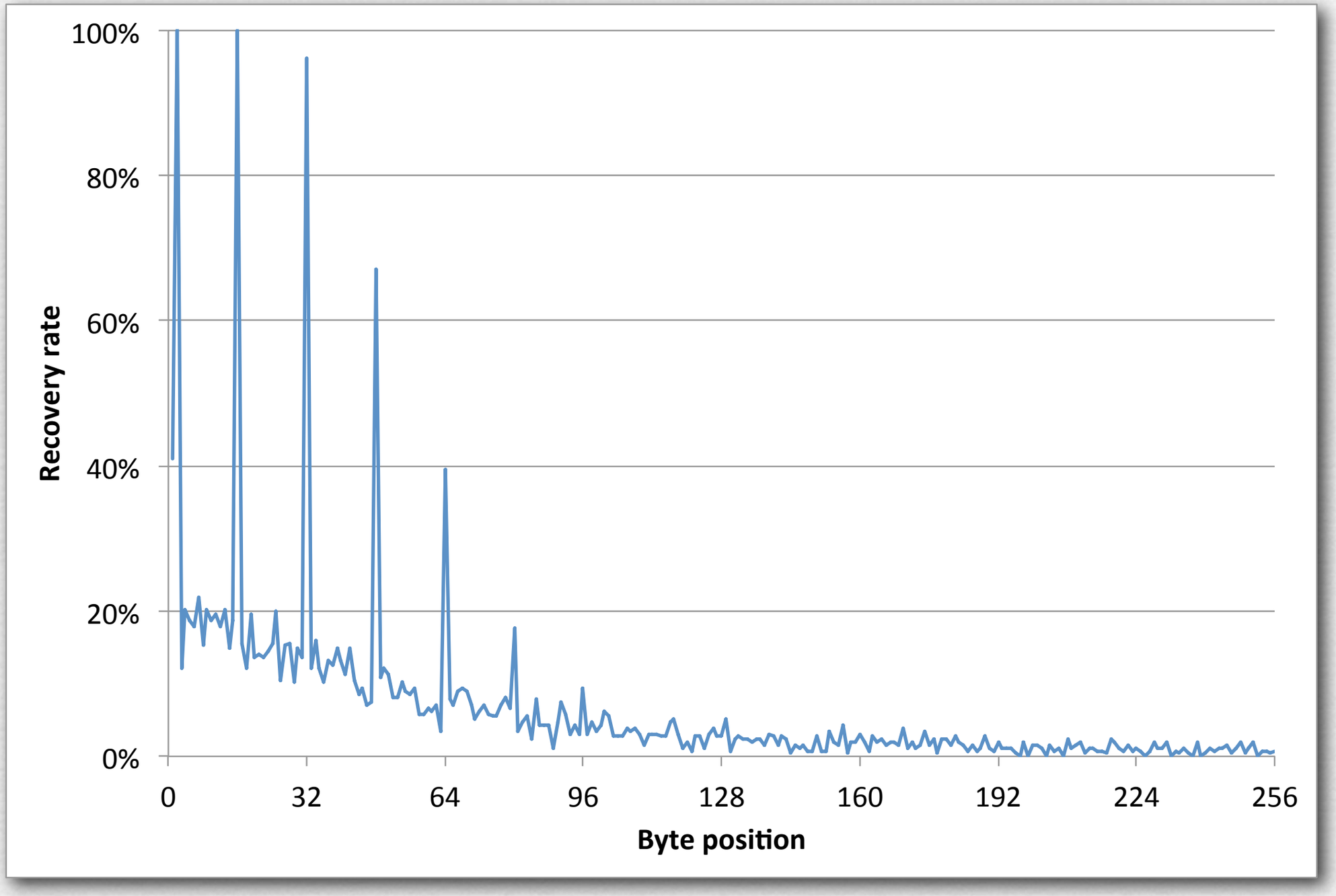


Success Probability
2^{22} Sessions

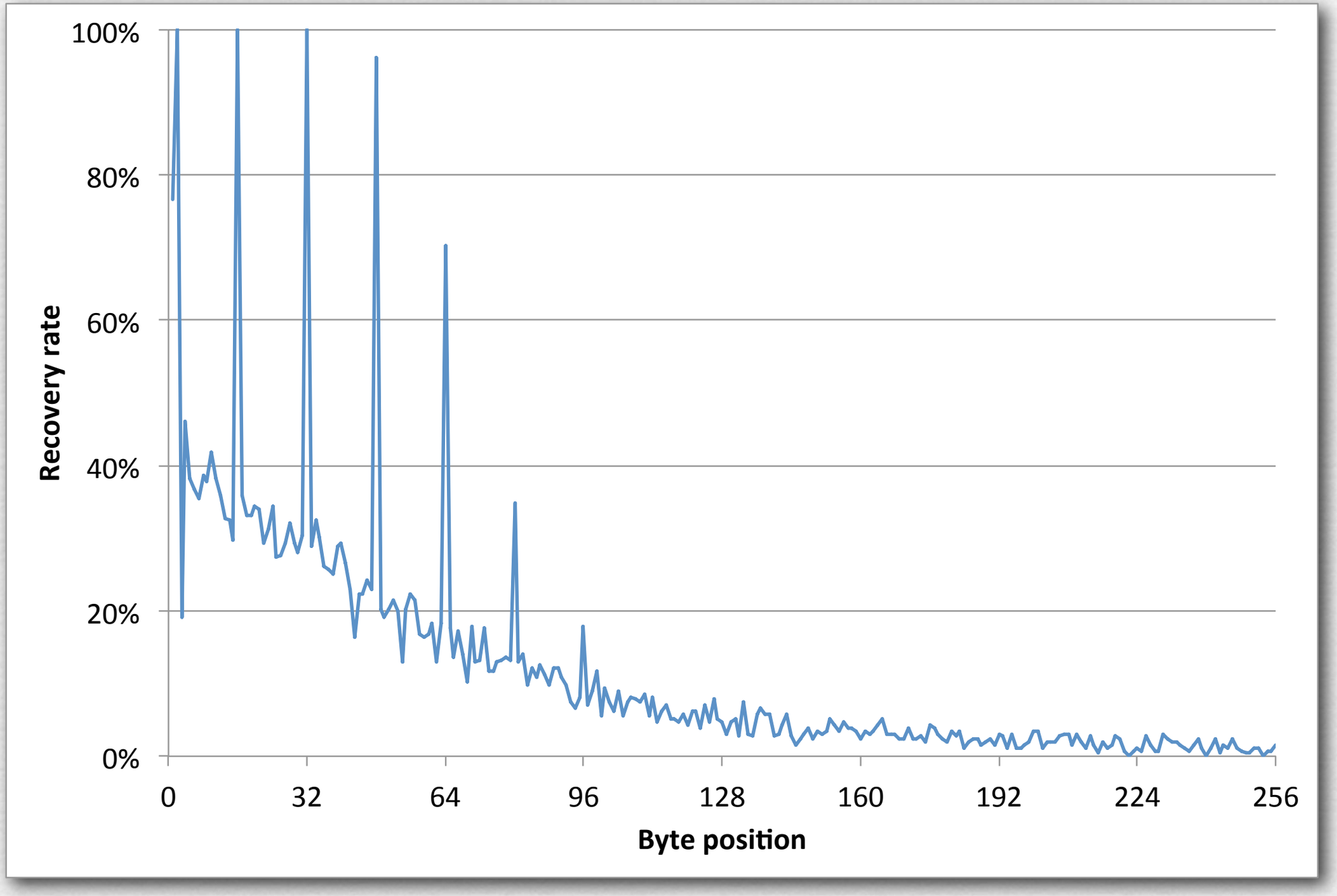
Information Security Group



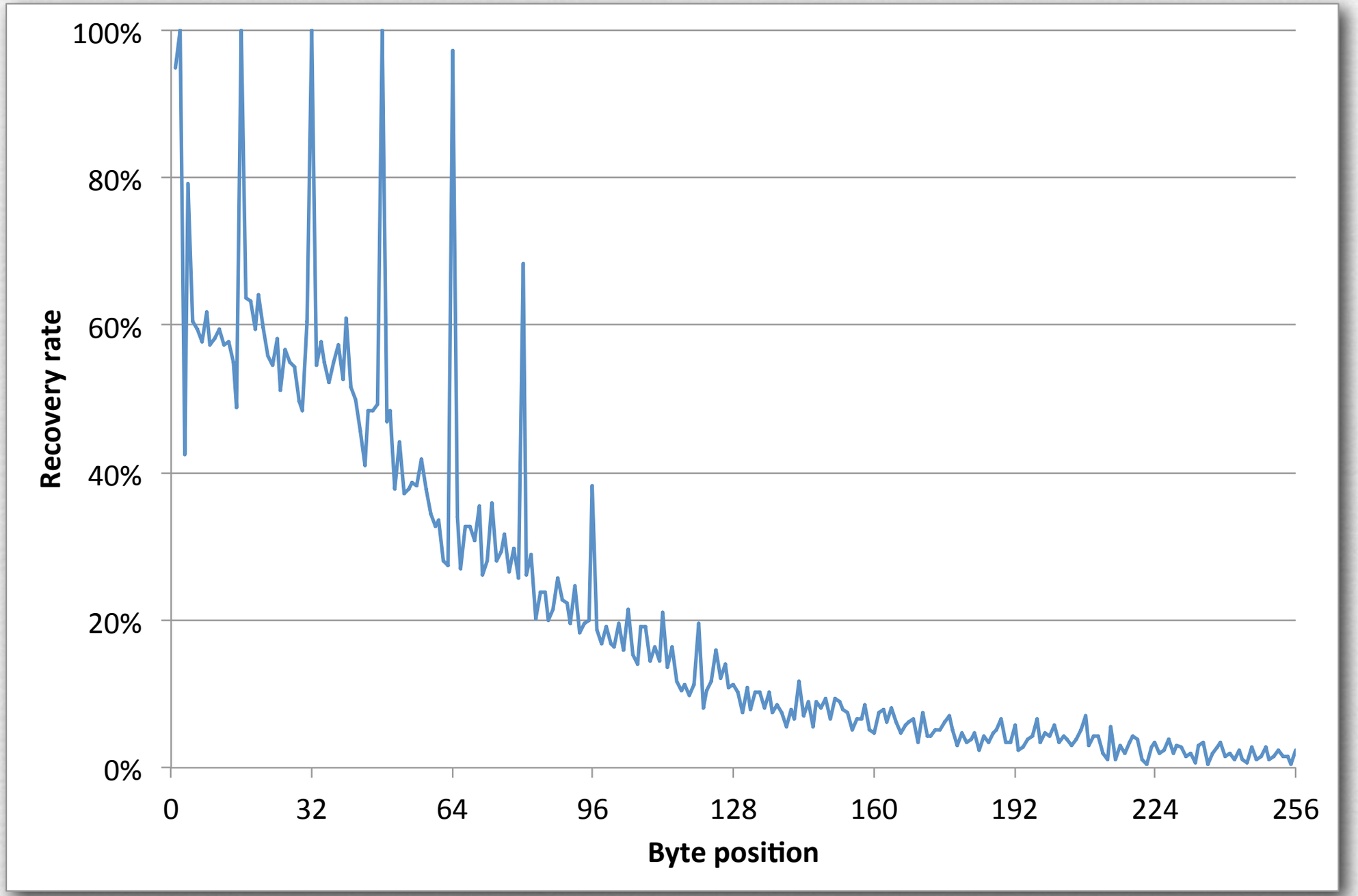
Success Probability
2^{23} Sessions



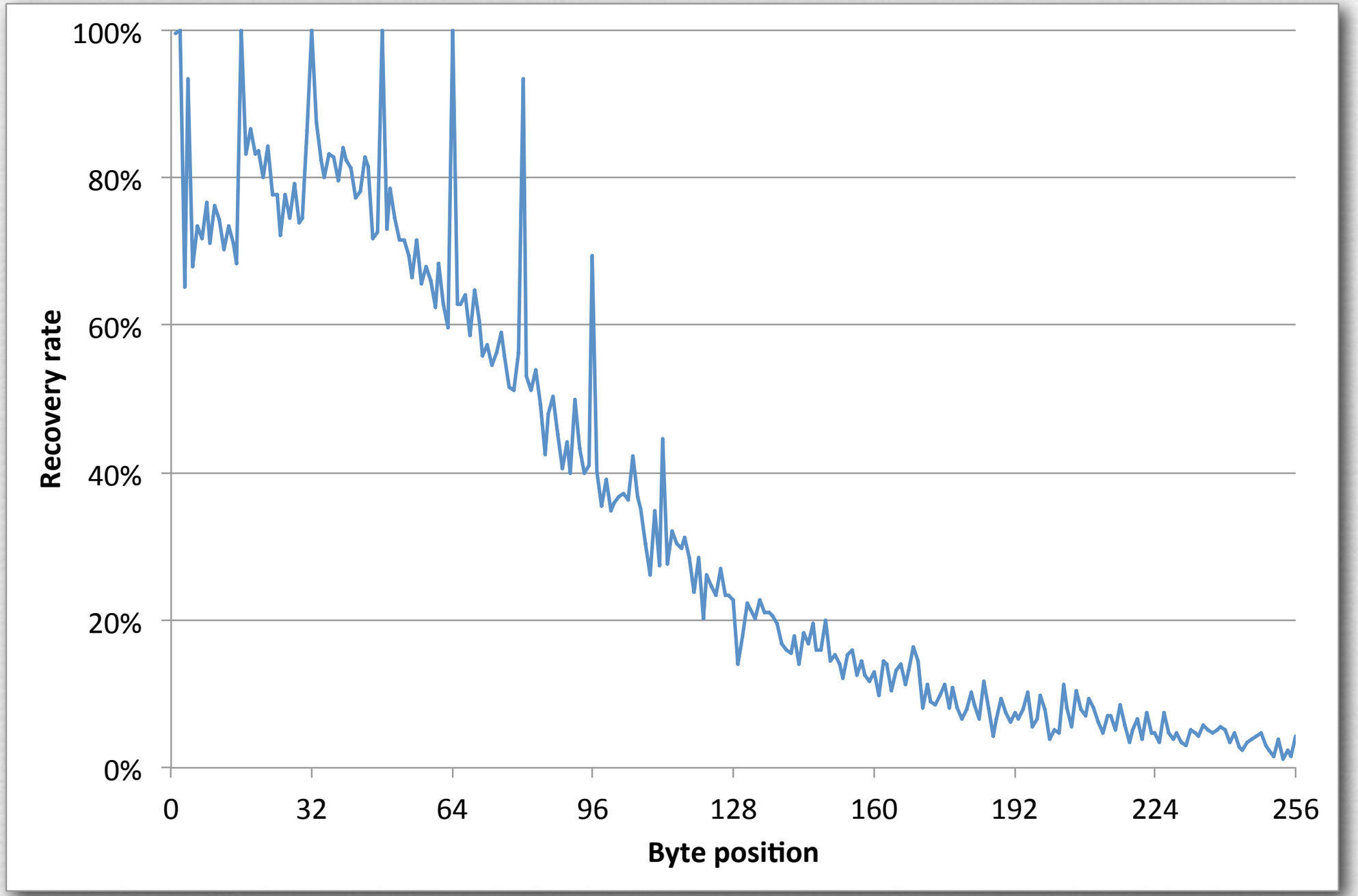
Success Probability
2^{24} Sessions



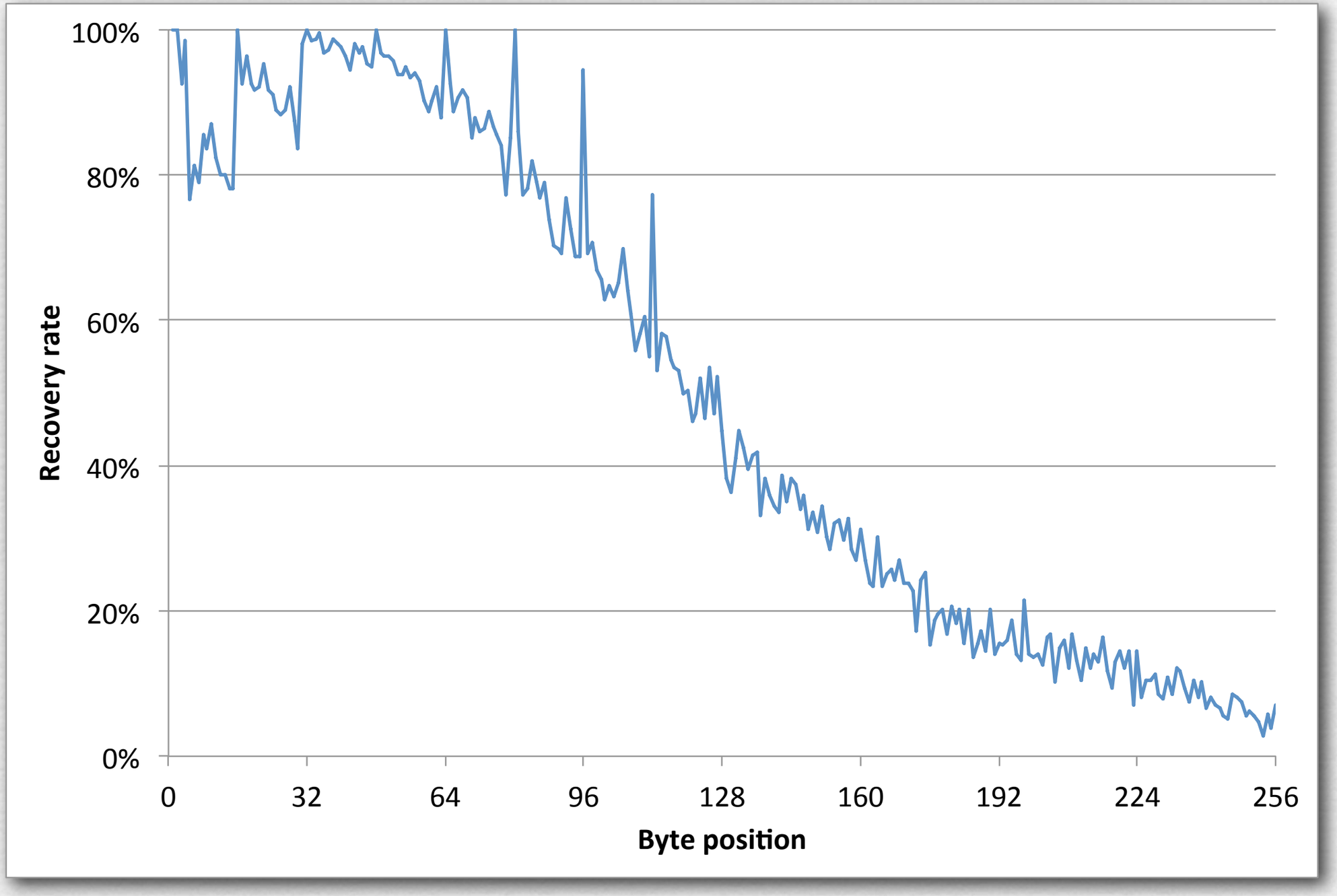
Success Probability
2^{25} Sessions



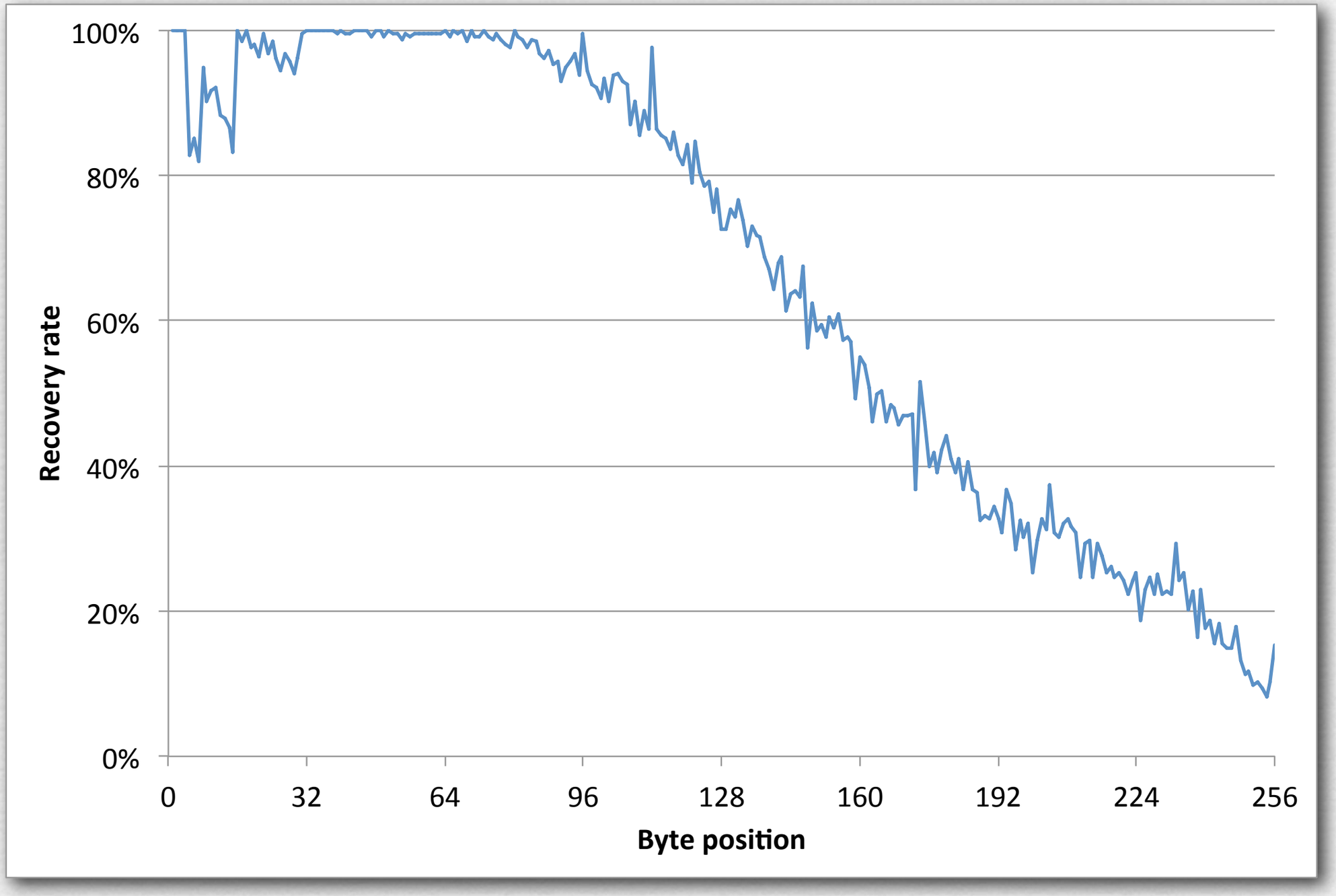
Success Probability
2^{26} Sessions



Success Probability
2^{27} Sessions

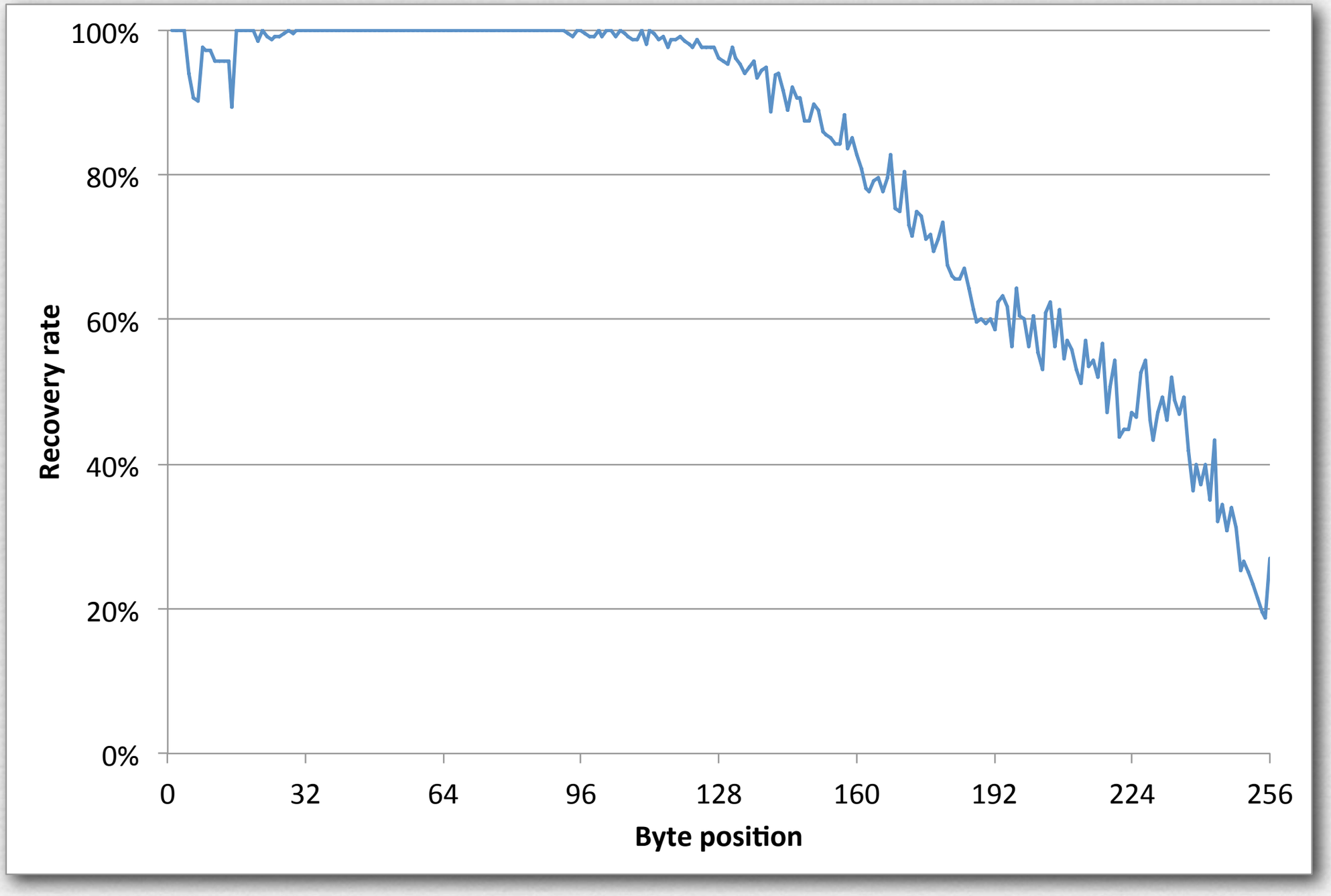


Success Probability
2^{28} Sessions

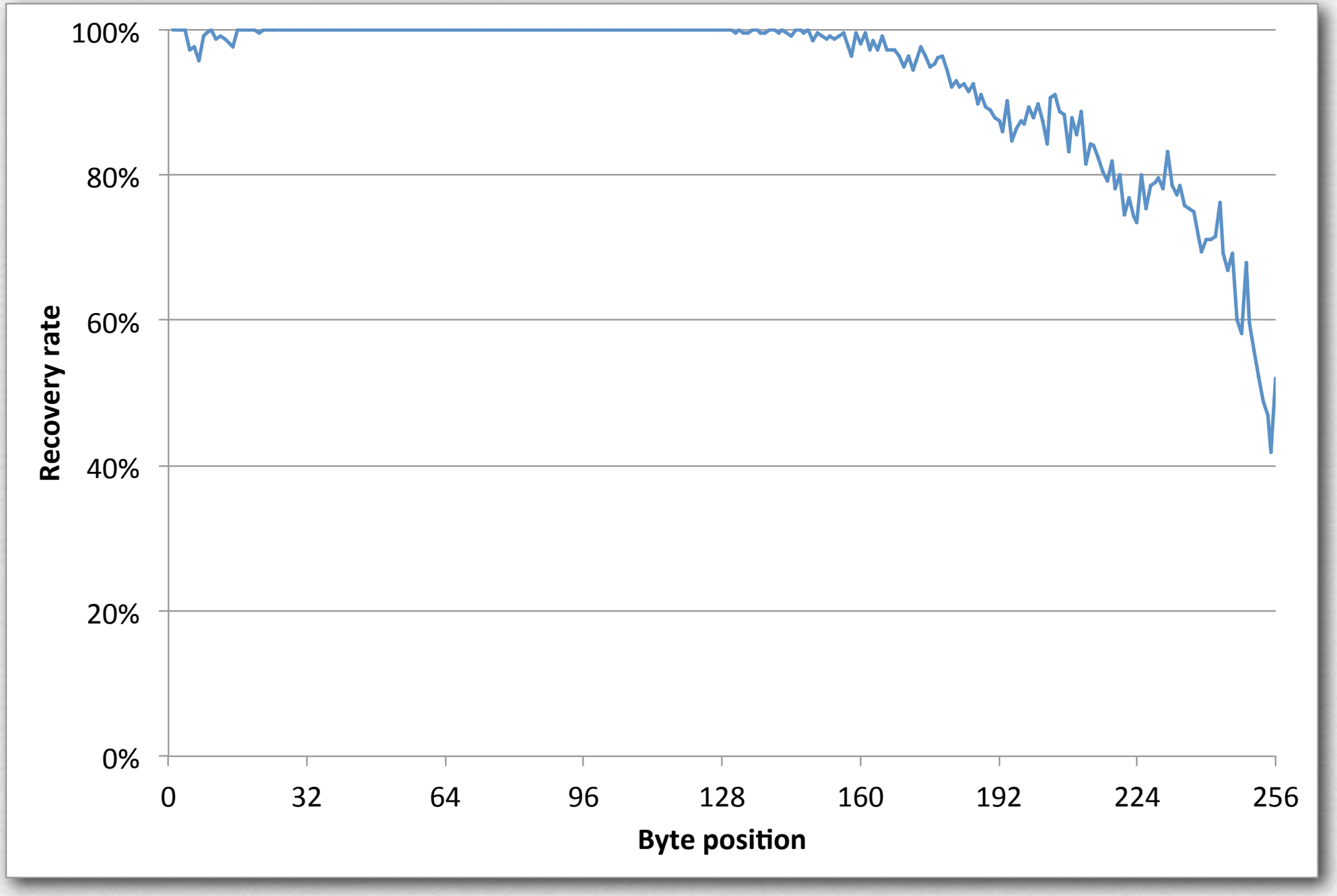


Success Probability
2^{29} Sessions

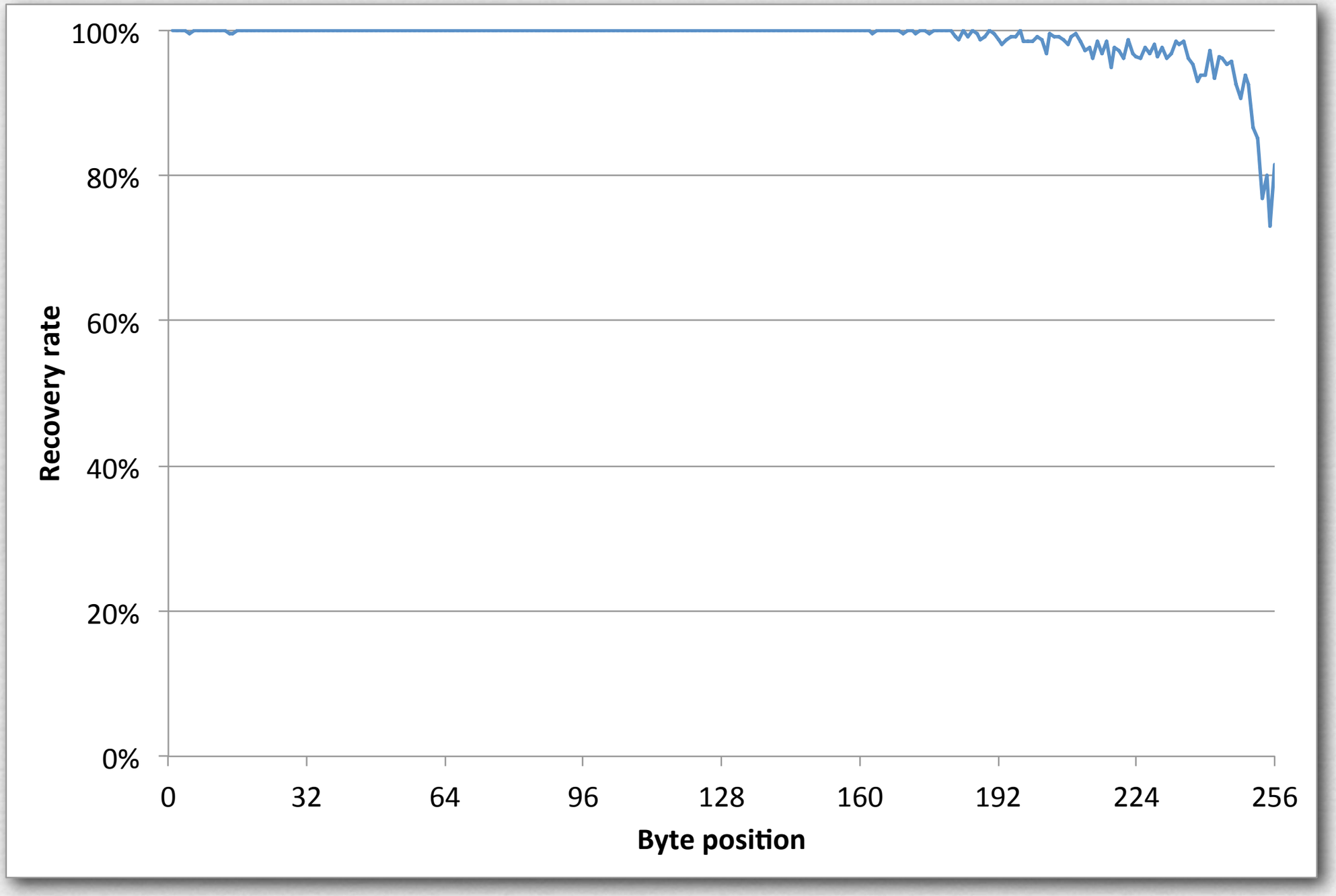
Information Security Group



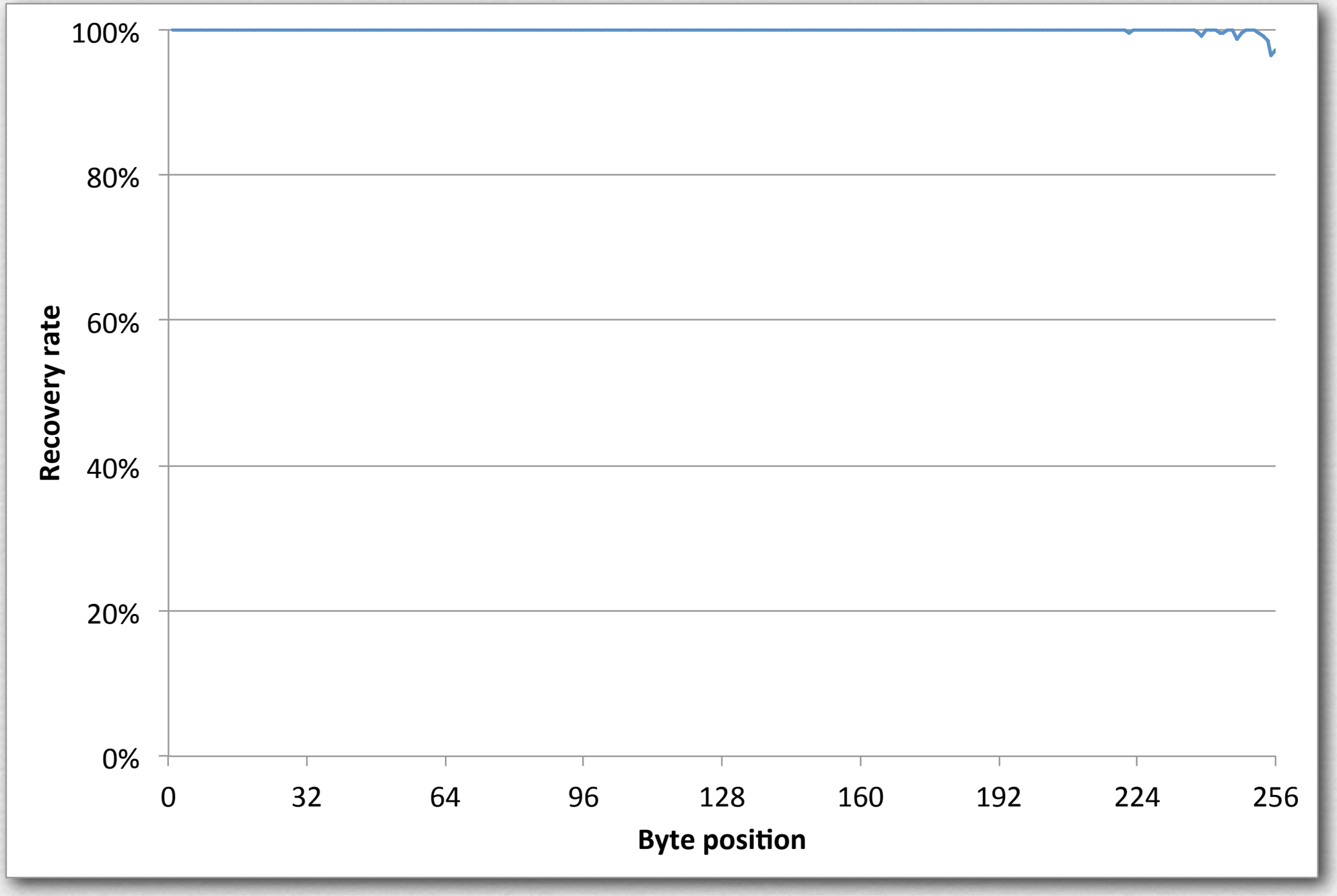
Success Probability
2^{30} Sessions



Success Probability
2^{31} Sessions



Success Probability
2^{32} Sessions



Second Attack

Double-byte
“long term” biases

+

⇒

TLS plaintext
recovery
(any bytes)

Second Attack

- Beyond byte position 256?

Double-byte "long term" biases +  ⇒ TLS plaintext recovery (any bytes)

Second Attack

- Beyond byte position 256?

Double-byte "long term" biases + 

⇒ TLS plaintext recovery (any bytes)

- Interested?

http://isg.rhul.ac.uk/tls/ Google TLS + RHUL

Second Attack

- Beyond byte position 256?

Double-byte "long term" biases +  ⇒ TLS plaintext recovery (any bytes)

- Interested?

http://isg.rhul.ac.uk/tls/ Google TLS + RHUL

Thank You!