Royal Holloway
University of London

Plaintext Recovery Attacks Against WPA/TKIP

Kenny Paterson, Bertram Poettering, Jacob Schuldt
Royal Holloway, University of London

The 21st International Workshop on Fast Software Encryption
March 4th, 2014

jacob.schuldt@rhul.ac.uk

Information Security Group

Agenda

Information Security Group

- Introduction to WPA/TKIP
- Biases in the WPA/TKIP keystreams
- Plaintext recovery attack for the repeated plaintext setting
- Exploiting TSCs for improved attacks
- Concluding remarks/open problems

Introduction to WPA/TKIP

- IEEE standards for wireless LAN encryption
  - 1999: WEP (Wired Equivalent Privacy)
  - 2003: WPA (WiFi Protected Access)
  - 2004: WPA2 (WiFi Protected Access 2)

Introduction to WPA/TKIP

Information Security Group

WEP

- Badly broken:
  - Key recovery attack based on RC4 weakness and construction of RC4 key from 24-but known IV and unknown, but fixed key
  - 10k~20k packets needed for key recovery

WPA

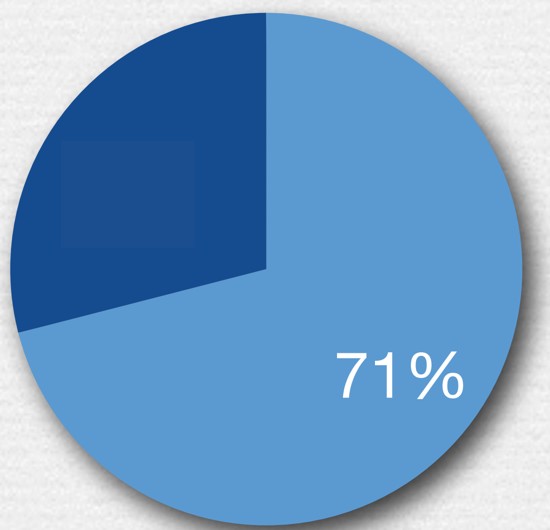
- Proposed by IEEE as an intermediate solution
  - Allows reuse of the hardware implementing WEP
  - Introduction of supposedly better per-frame RC4 key through the Temporal Key Integrity Protocol (TKIP)

WPA2

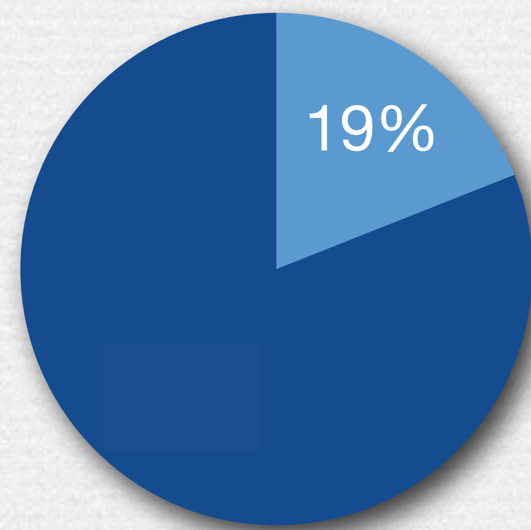
- Introduces a stronger cryptographic solution based on AES-CCM
  - (Includes optional support for TKIP)

Introduction to WPA/TKIP

- WPA was only intended as a temporary fix
- However, WPA is still in widespread use today
  - Vanhoef-Piessens (2013) surveyed 6803 wireless networks:



Permit WPA/TKIP



Only allow WPA/TKIP

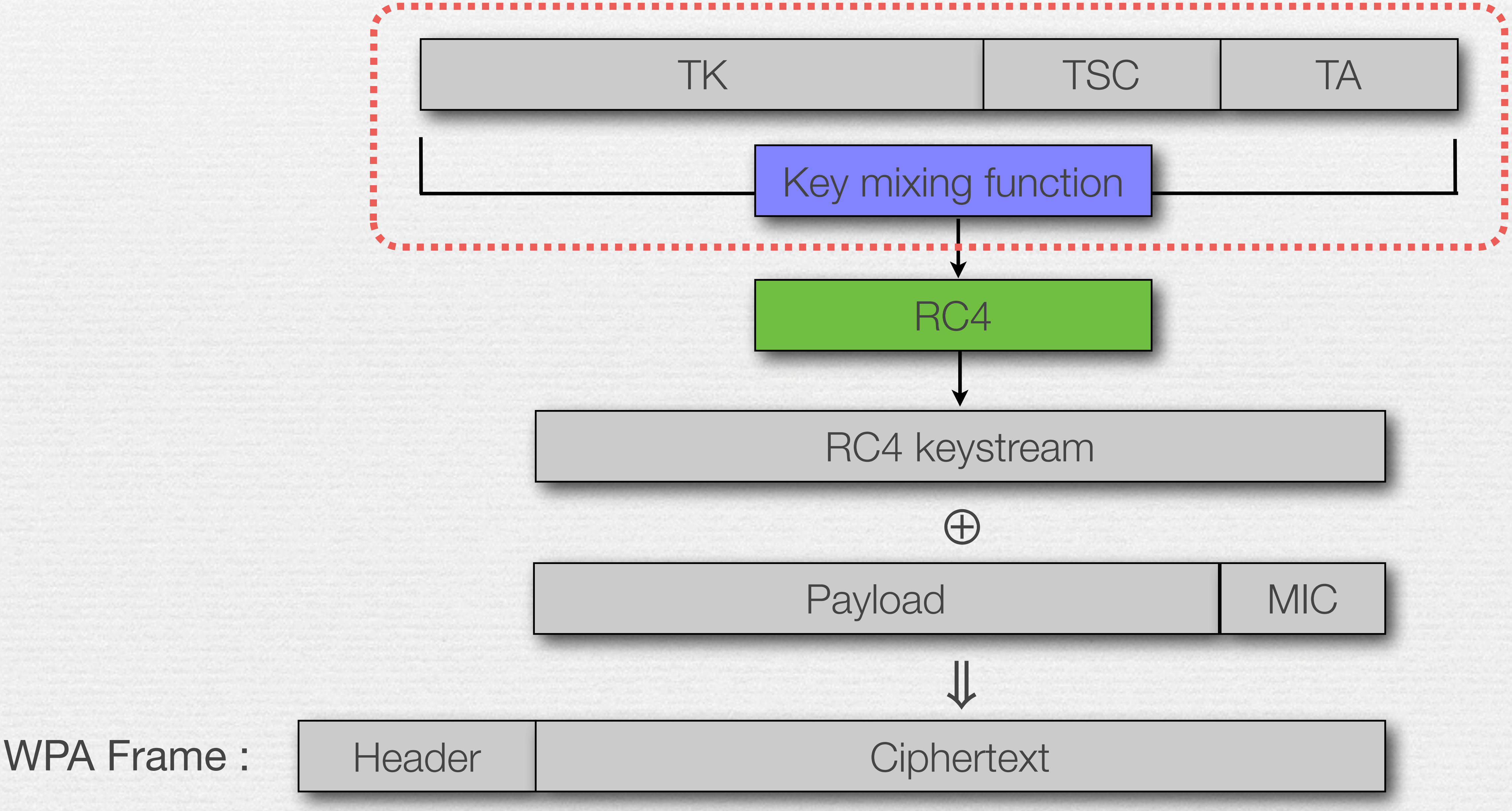
- This makes the continued analysis of WPA/TKIP worthwhile

Overview of WPA/TKIP Encryption

TK : Temporal key (128 bits)

TA : Sender Address (48 bits)

TSC : TKIP Sequence Counter (48 bits)

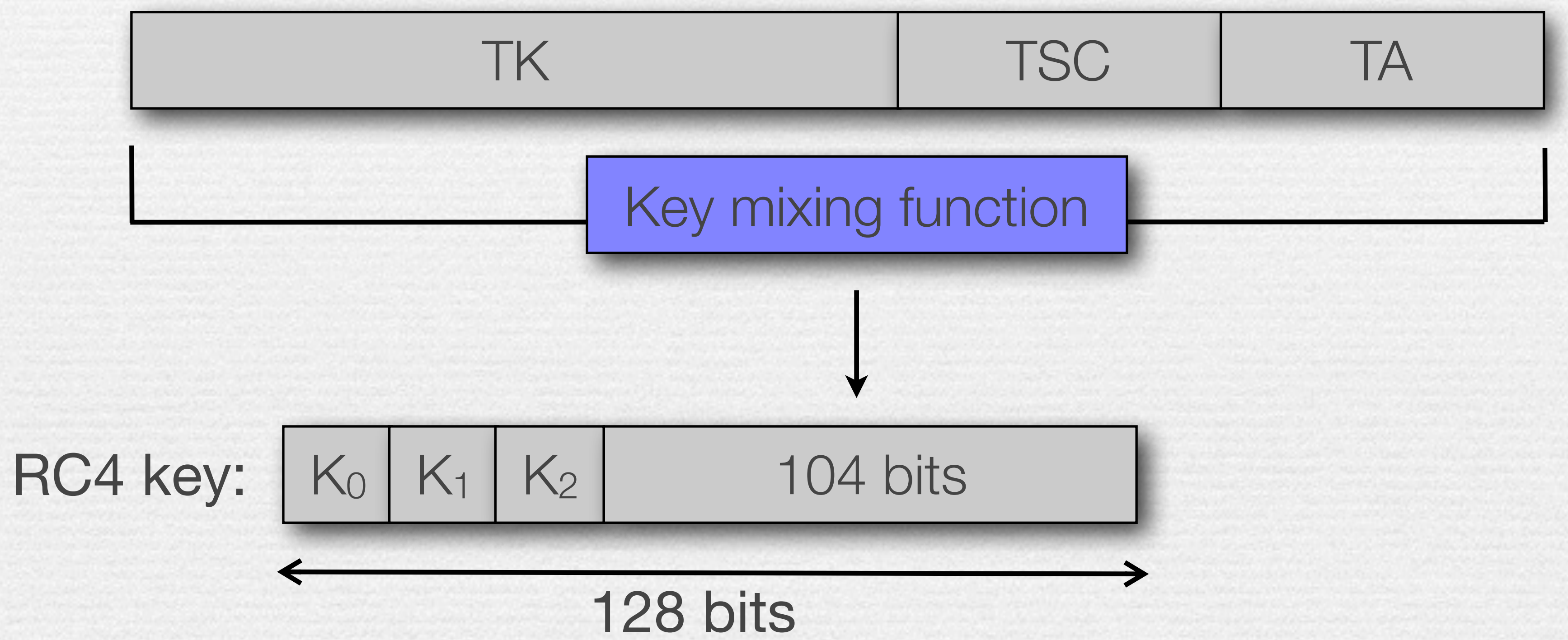


Overview of WPA/TKIP Encryption

TK : Temporal key (128 bits)

TA : Sender Address (48 bits)

TSC : TKIP Sequence Counter (48 bits)



$K_0 = TSC_1$

$K_1 = (TSC_1 \mid 0x20) \,\&\, 0x7f$

$K_2 = TSC_0$

<u>TSC_0, TSC_1</u>

Two least significant bytes of TSC

Previous Attacks on WPA/TKIP

Information Security Group

- Tews-Beck (2009):
  - Rate-limited plaintext recovery
  - Active attack based on chop-chop method for recovering plaintext
  - Requires support for alternative QoS channels to by-pass anti-replay protection
  - Rate-limited since correctness of plaintext guess is indicated by MIC verification failure, and only 2 failures per minute are tolerated

- Sepehrdad-Vaudenay-Vuagnoux (2011):
  - Statistical key recovery attack using 2^{38} known plain texts and 2^{96} operations

New Plaintext Recovery Attacks

RC4 with Random 128-bit Keys

- Recent work* has shown that RC4 with random 128-bit keys has significant biases in all of its initial keystream bytes

- Such biases enable plaintext recovery if sufficiently many encryptions of the same plaintext are available
  - Uses simple Bayesian statistical analysis
  - Applicable in multi-session or broadcast attack scenario

* AlFardan-Berstein-Paterson-Poettering-Schuldt (2013); Isobe-Ohigashi-Watanabe-Morii (2013)

Plaintext Recovery

Information Security Group

Encryptions of plaintext under different keys

Plaintext candidate byte P_r

Z_r : keystream byte at position r

r

C_1

C_2

C_3

⋮

C_n

$P_r \oplus$

$P_r \oplus$

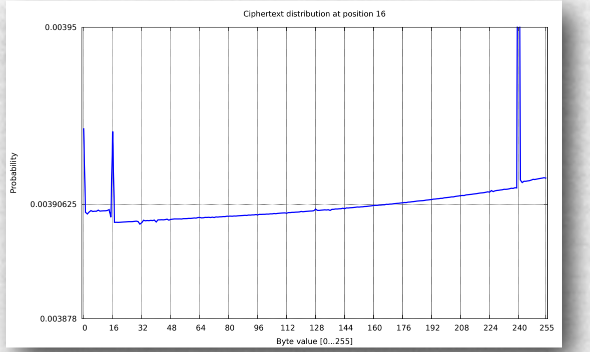
$P_r \oplus$

⋮

$P_r \oplus$

Induced distribution on Z_r

combine with known distribution of Z_r



$\Downarrow$

Likelihood of P_r being correct plaintext byte

Recovery algorithm:
Compute most likely plaintext byte

Applications

Information Security Group

- Technique successfully applied to RC4 as used in SSL/TLS by AlFardan-Bernstein-Paterson-Schuldt (2013)
  - Attack realizable in TLS context using client-side Javascript, resulting in session cookie recovery
  - (In practice, a version of the attack exploiting Fluhrer-McGrew double-byte biases is preferable)
- Applicable to RC4 with WPA/TKIP keys?
  - Every frame has a new key i.e. naturally close to the broadcast attack setting
    - Repeated encryption of the same target plaintext still required
  - WPA/TKIP specific biases?

Biases in WPA/TKIP Keystreams

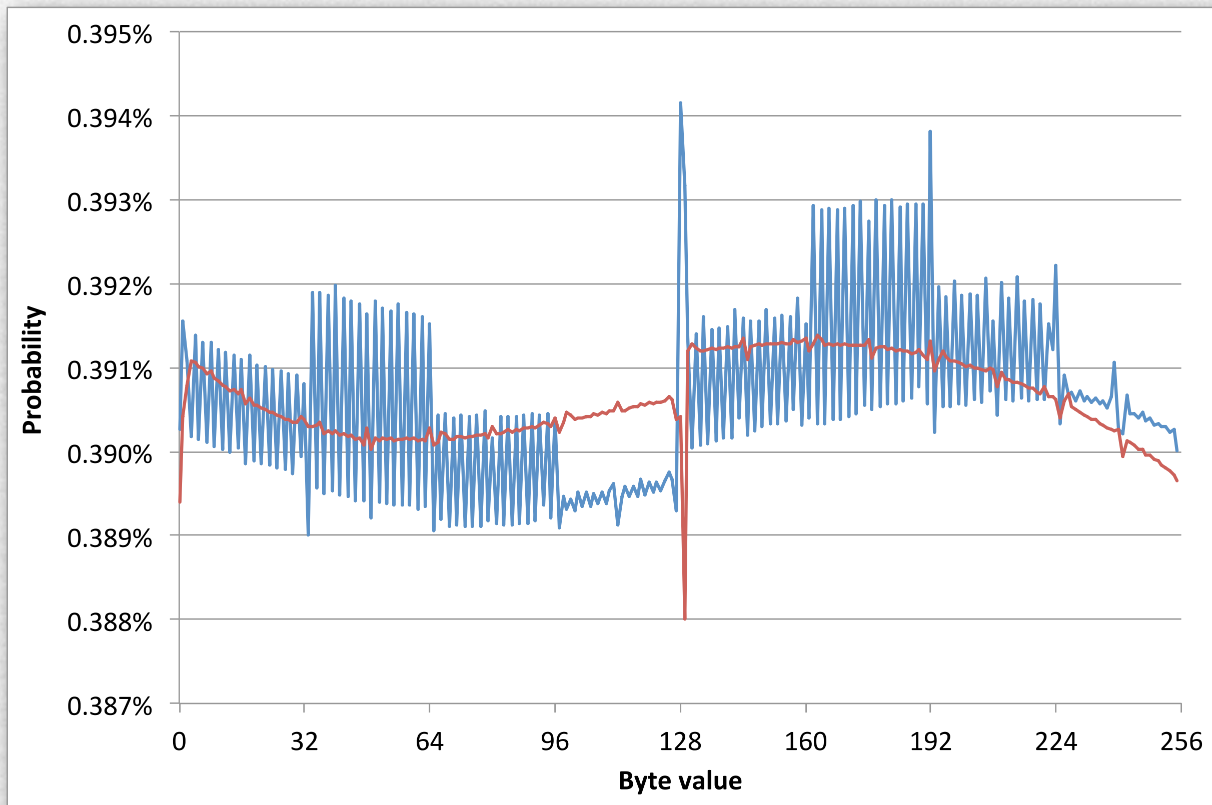
- Recall that WPA/TKIP keys have additional structure compared to random keys:

$$K_0 = TSC_1$$
$$K_1 = (TSC_1 \mid 0x20) \ \& \ 0x7f$$
$$K_2 = TSC_0$$

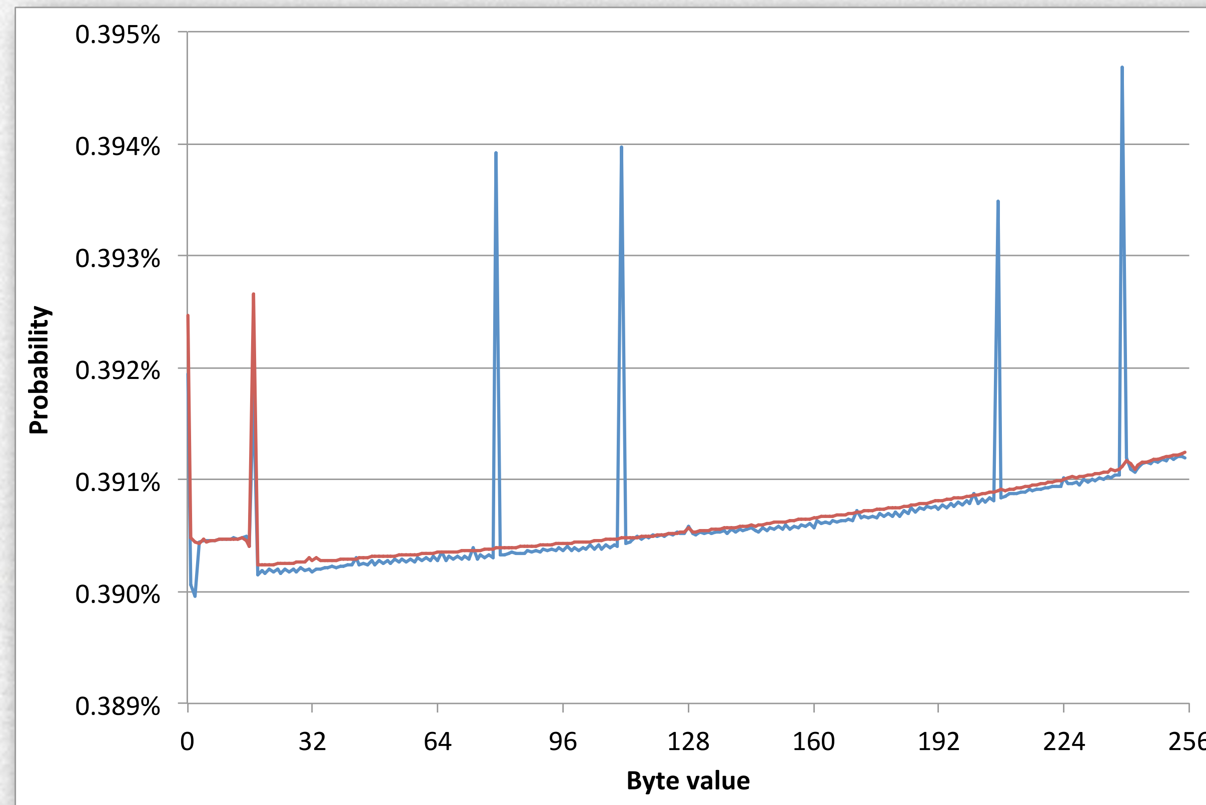
- This structure leads to significant changes in the biases in the RC4 keystream compared to random keys

Biases in WPA/TKIP: Keystream Byte 1 and 17

Keystream byte 1



Keystream byte 17

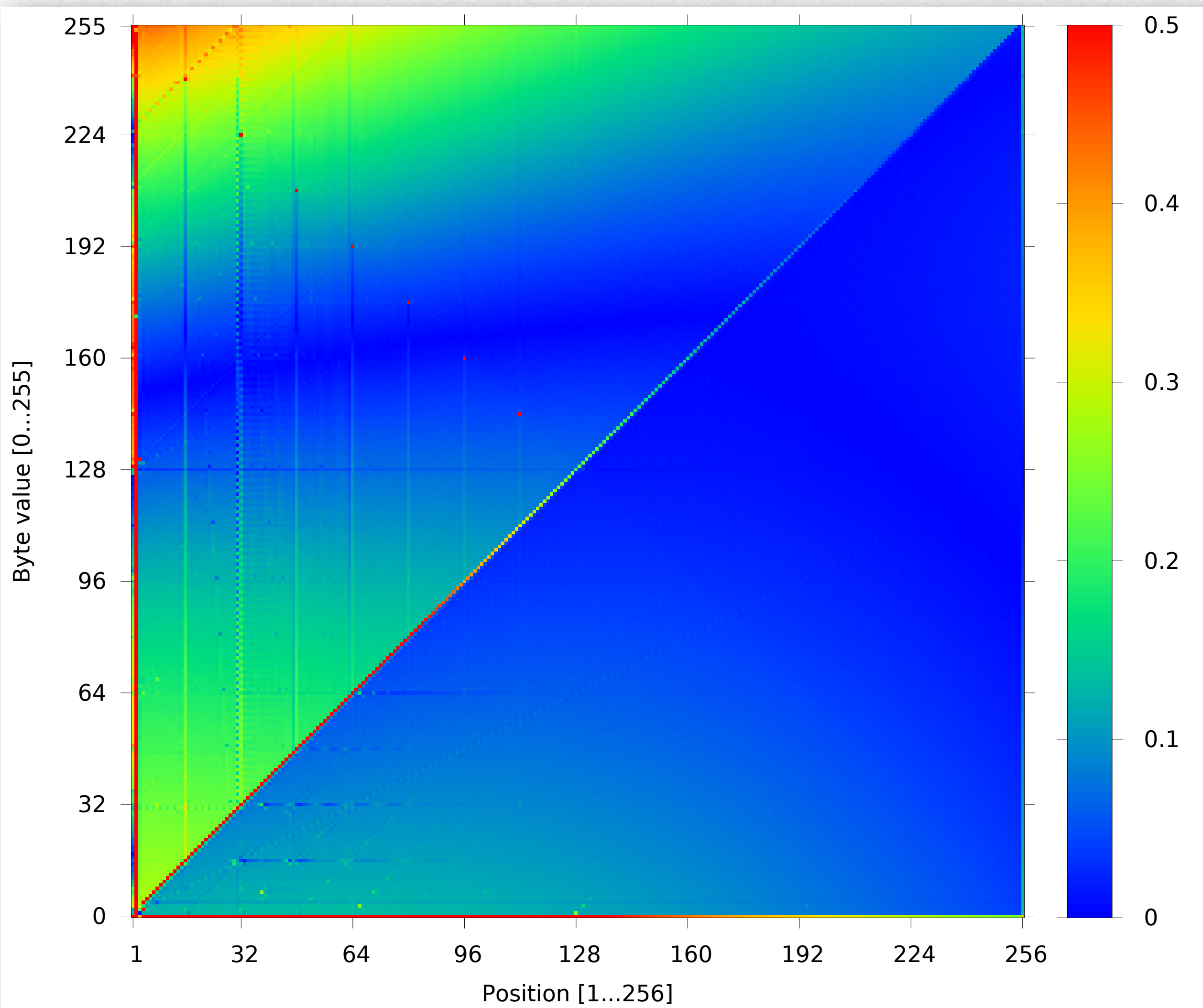


WPA/TKIP RC4 keys

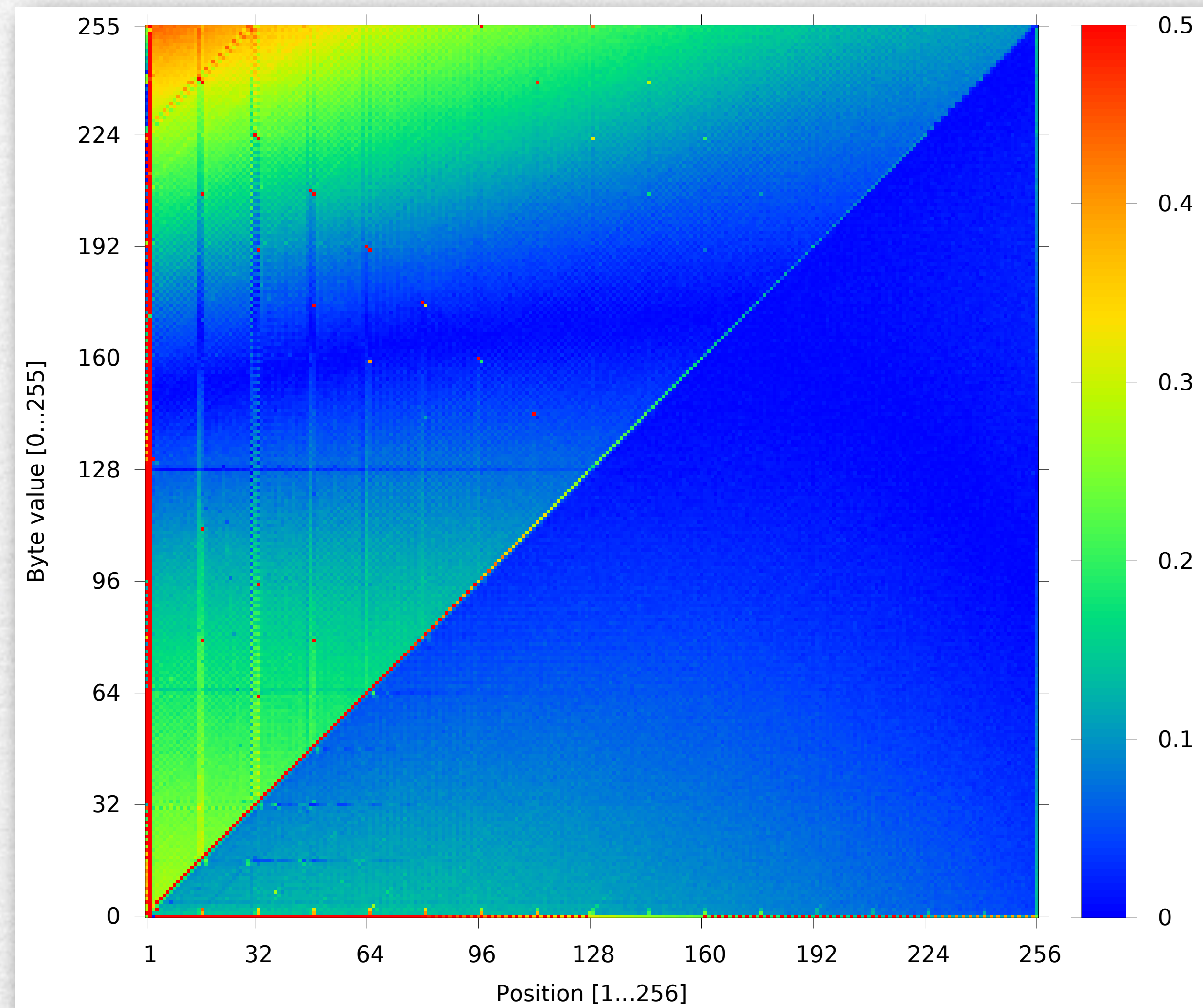
Random RC4 keys

Comparison with Biases for 128-bit Random RC4 Keys

Random RC4 keys

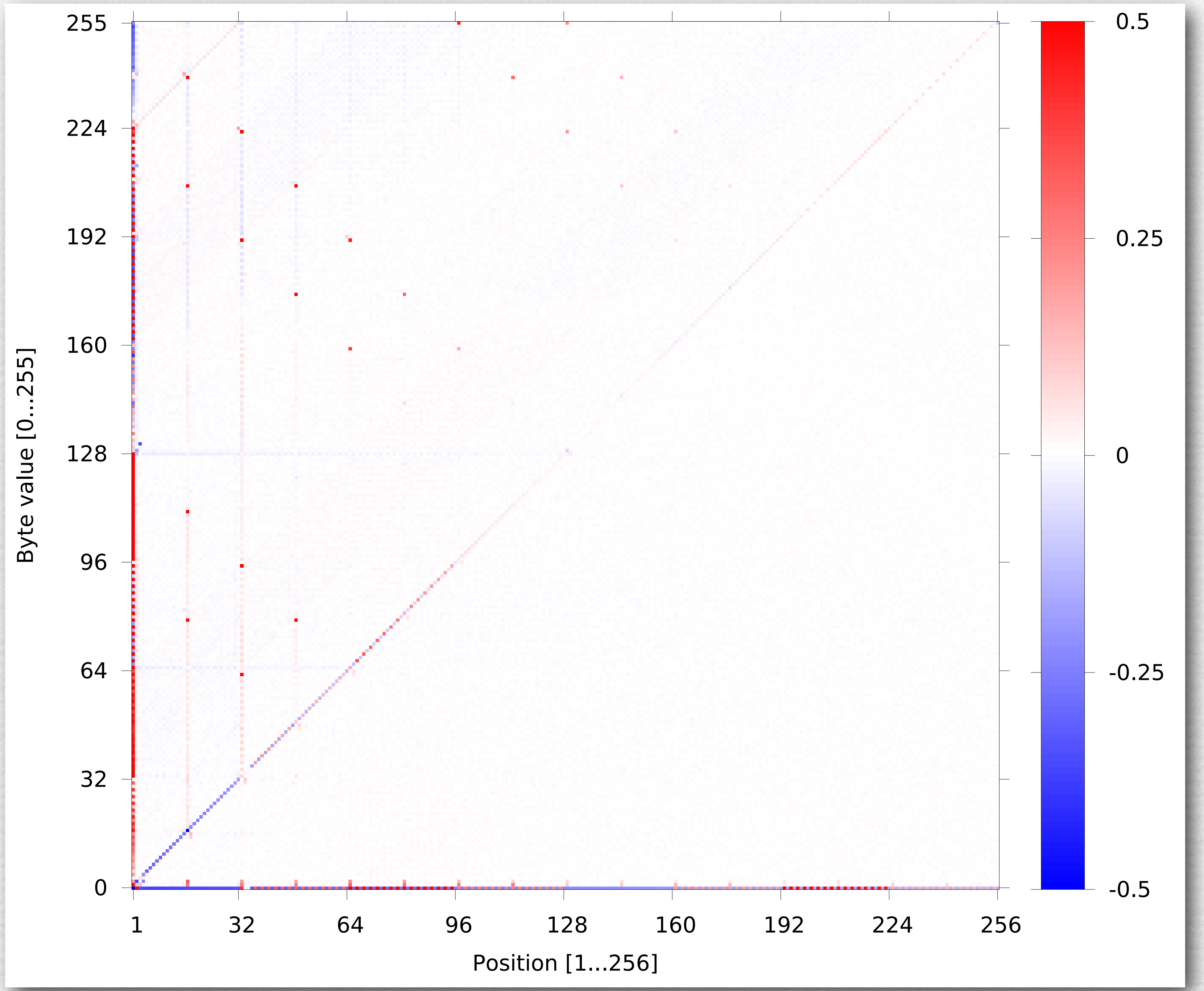


WPA/TKIP keys

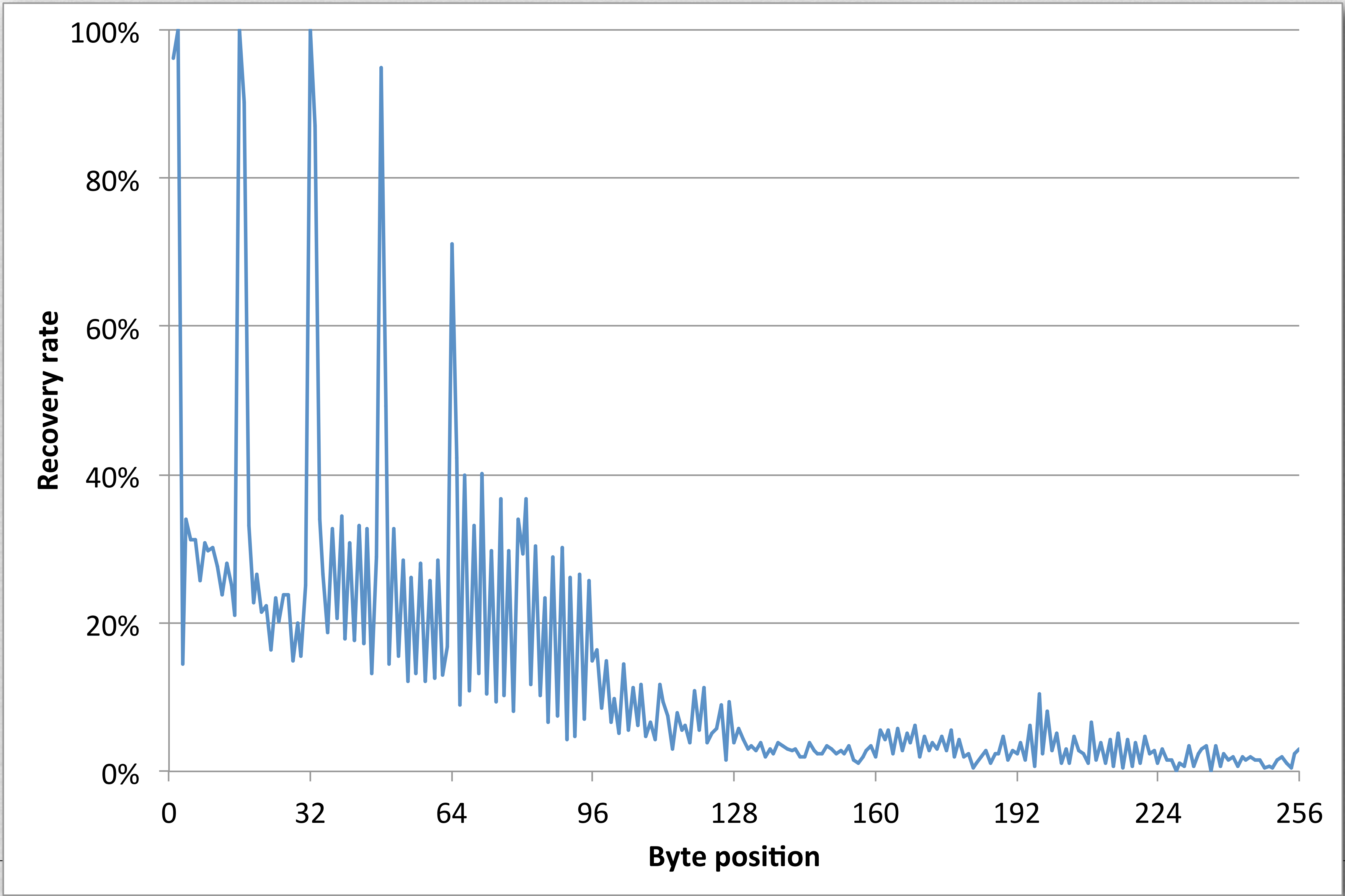


Color encoding: absolute strength of bias × 2^{16}

Comparison with Biases for 128-bit Random RC4 Keys



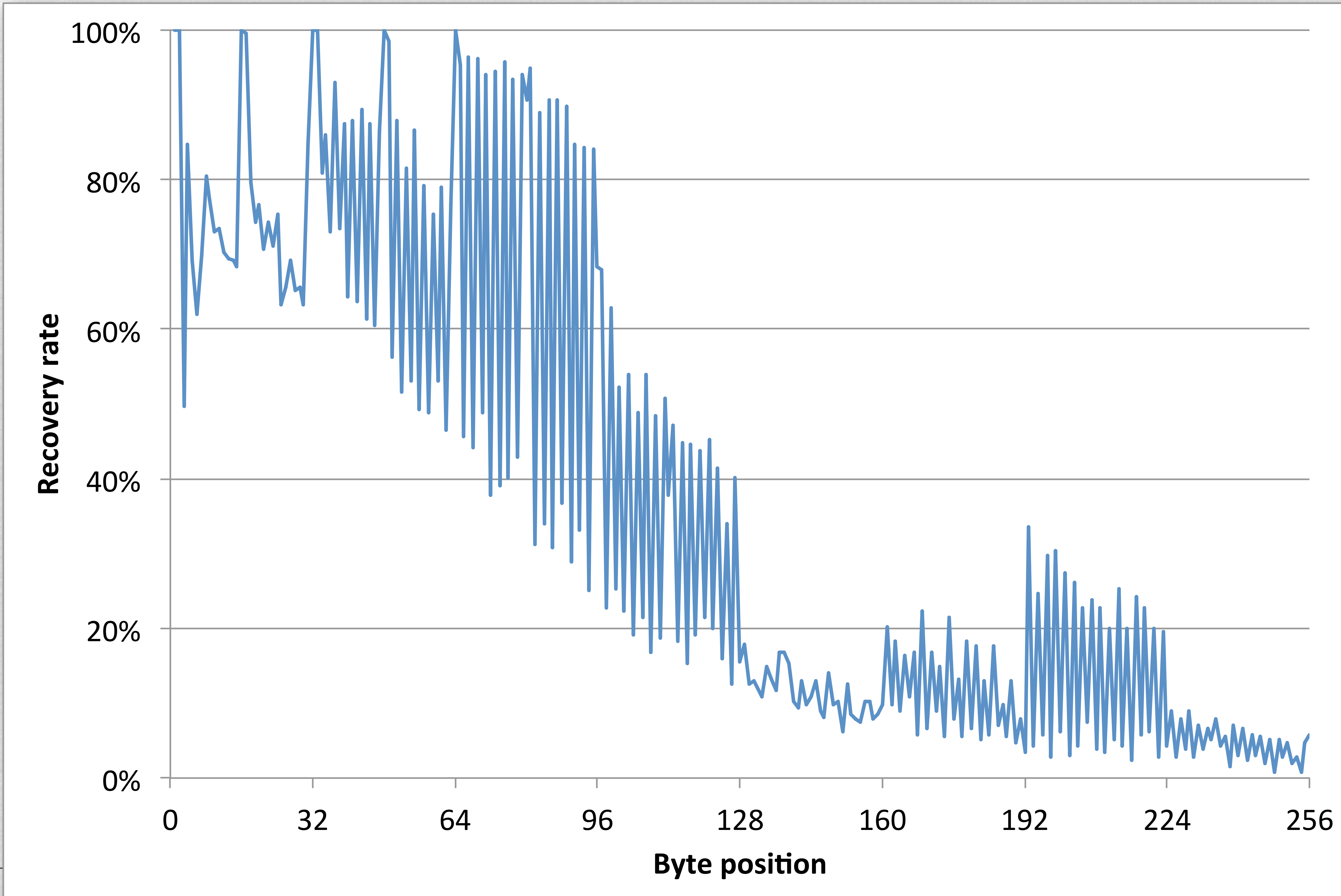
Plaintext Recovery Rate
2^{24} Frames



Information Security Group

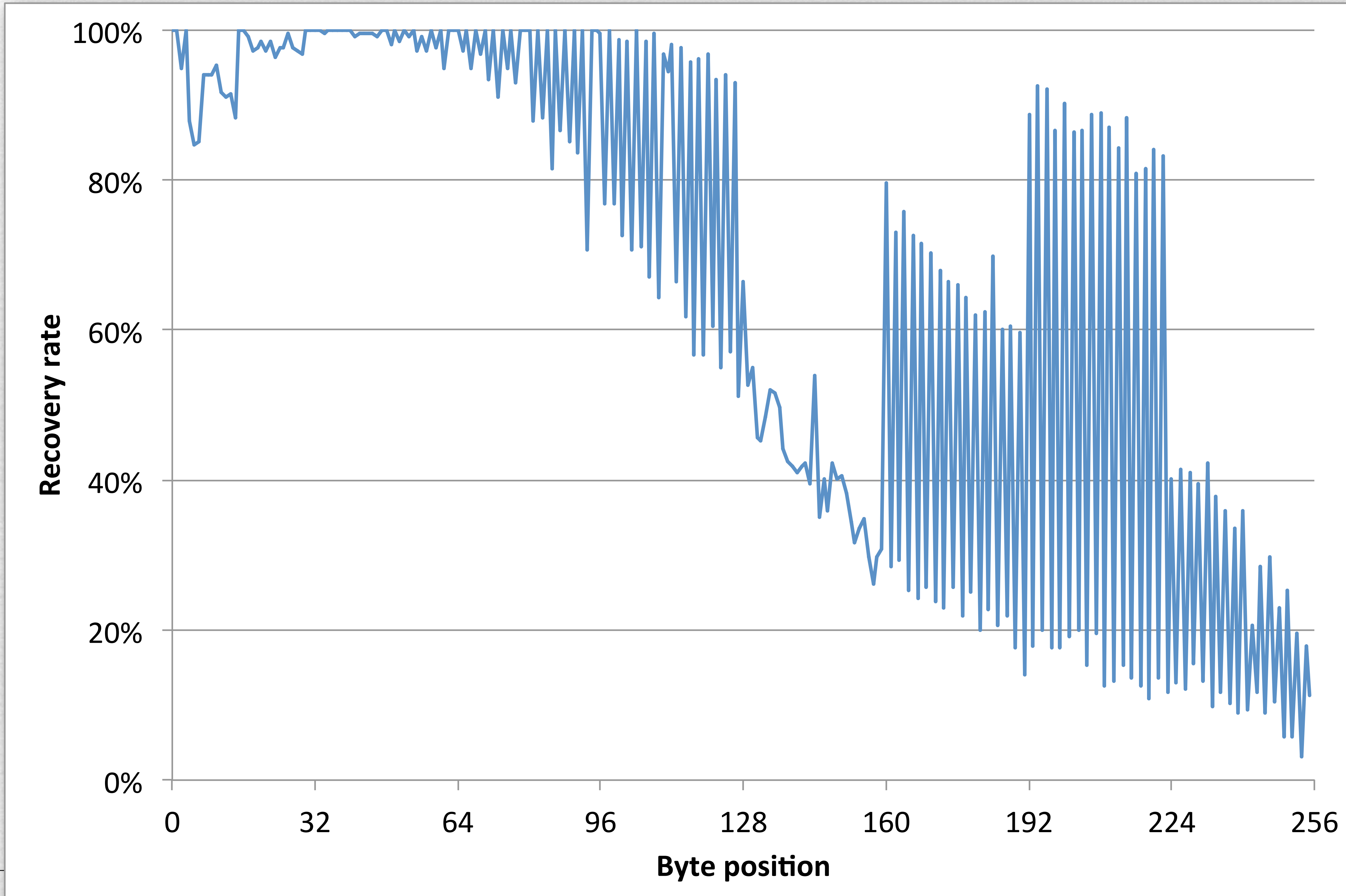
Plaintext Recovery Rate
2^{26} Frames

Information Security Group



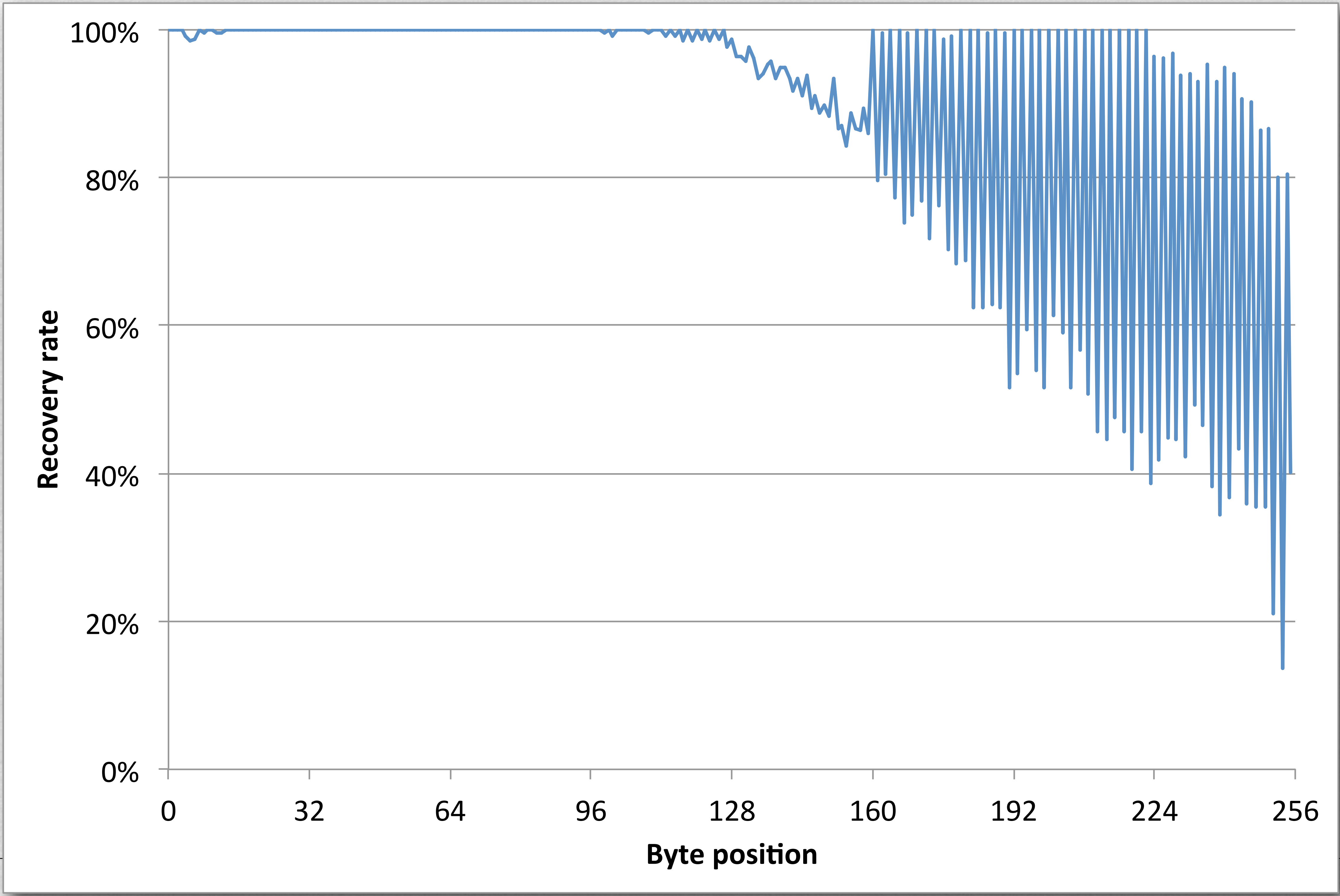
Plaintext Recovery Rate
2^{28} Frames

Information Security Group



Plaintext Recovery Rate
2^{30} Frames

Information Security Group



Exploiting TSCs

Exploiting TSC Information

- Again, recall the special structure of WPA/TKIP keys:

K_0 = TSC_1

K_1 = $(TSC_1 \mid 0x20) \& 0x7f$

K_2 = TSC_0

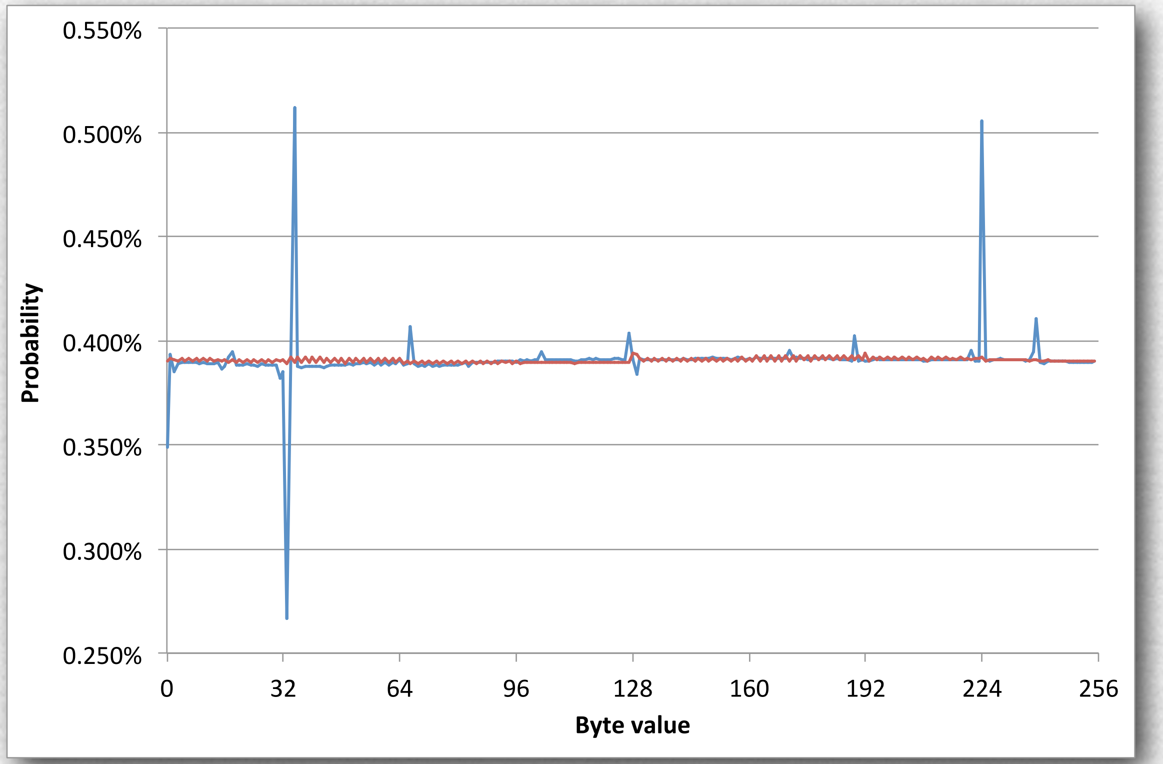
- Idea: identify and exploit (TSC_0, TSC_1)-specific biases

- Plaintext recovery attack based (TSC_0, TSC_1)-specific biases:

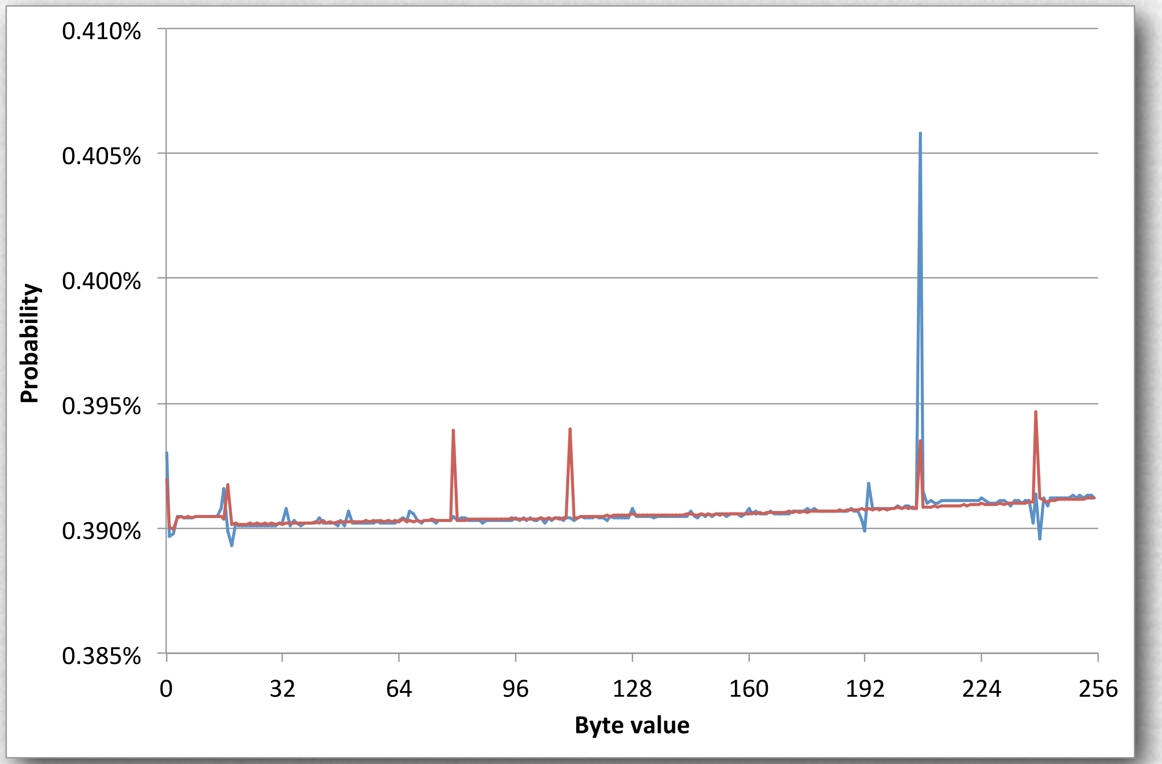
1. Group ciphertexts into 2^{16} groups according to (TSC_0, TSC_1) value
2. Carry out likelihood analysis for each group using appropriate keystream distribution
3. Combine likelihoods across groups to recover plaintext

Existence of Large (TSC_0, TSC_1)-specific Biases

(TSC_0, TSC_1) = (0x00, 0x00)



Keystream byte 1



Keystream byte 17

(TSC_0, TSC_1)-specific RC4 keys

RC4 keys with random (TSC_0, TSC_1)

Computational Requirements for (TSC_0, TSC_1)-specific Attack

- Problem:
  - A very large number of keystreams are required to get an accurate estimate for the (TSC_0, TSC_1)-specific keystream distributions

Minimum:	2^{32} keystreams per (TSC_0, TSC_1) pair	$\times$	2^{16} (TSC_0, TSC_1) pairs	$=$	2^{48} Keystreams	$=$	$\sim 2^{14}$ core days
Ideally:	2^{40} keystreams per (TSC_0, TSC_1) pair	$\times$	2^{16} (TSC_0, TSC_1) pairs	$=$	2^{56} Keystreams	$=$	$\sim 2^{22}$ core days

$\sim 2^{34}$ keystreams per core day

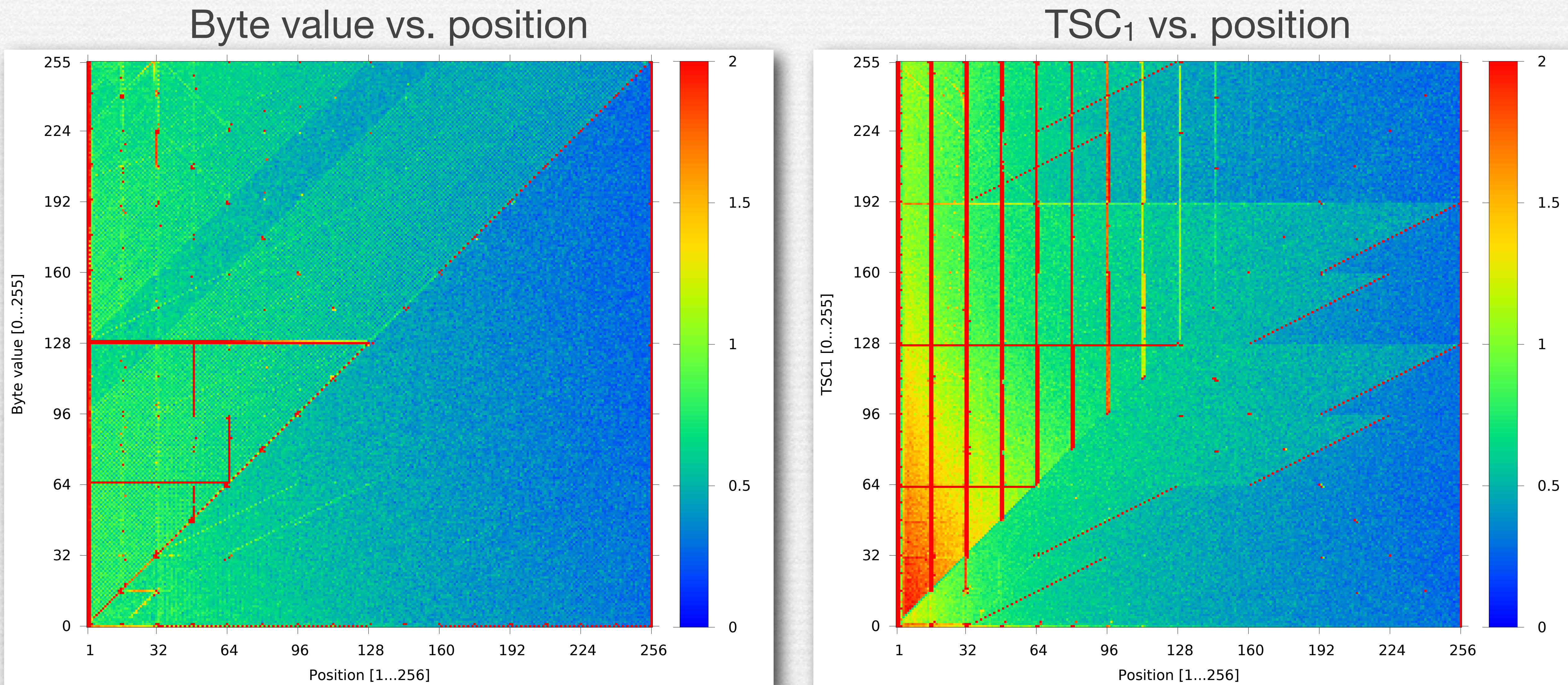
TSC_0 Aggregation

- TSC_1 is used to compute two key bytes; TSC_0 only one:

$$K_0 = TSC_1$$
$$K_1 = (TSC_1 \mathbin{\&} 0x20) \mid 0x7f$$
$$K_2 = TSC_0$$

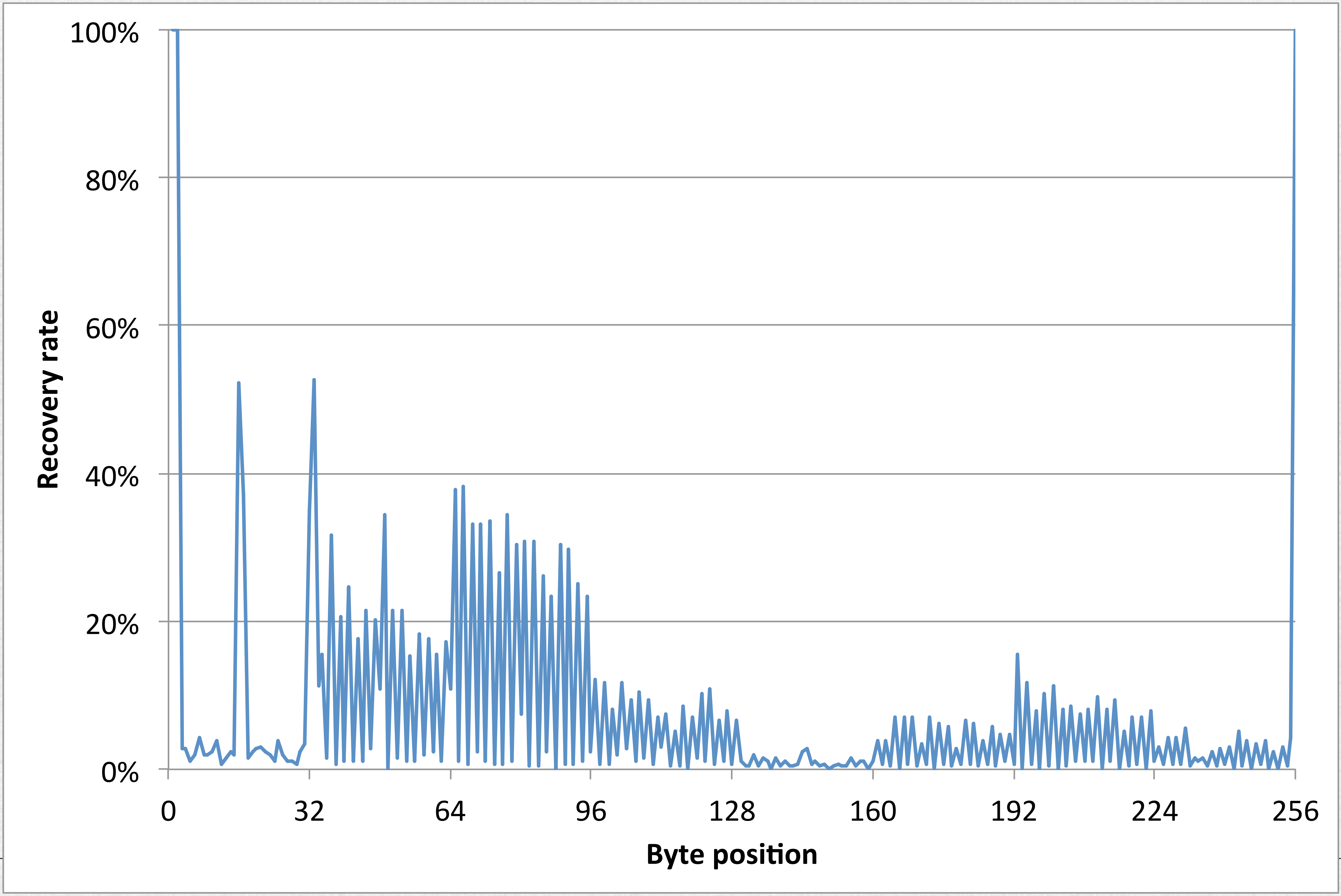
- Hence, we might expect significant biases to be strongly correlated with TSC_1
  - Experiments confirm this
- Alternative plaintext recovery attack
  - Group ciphertexts according to TSC_1 and carry out likelihood analysis based on TSC_1-specific keystream estimates
  - Reduced required number of keystreams with a factor of 2^8

Location of Large TSC_1 Specific Biases

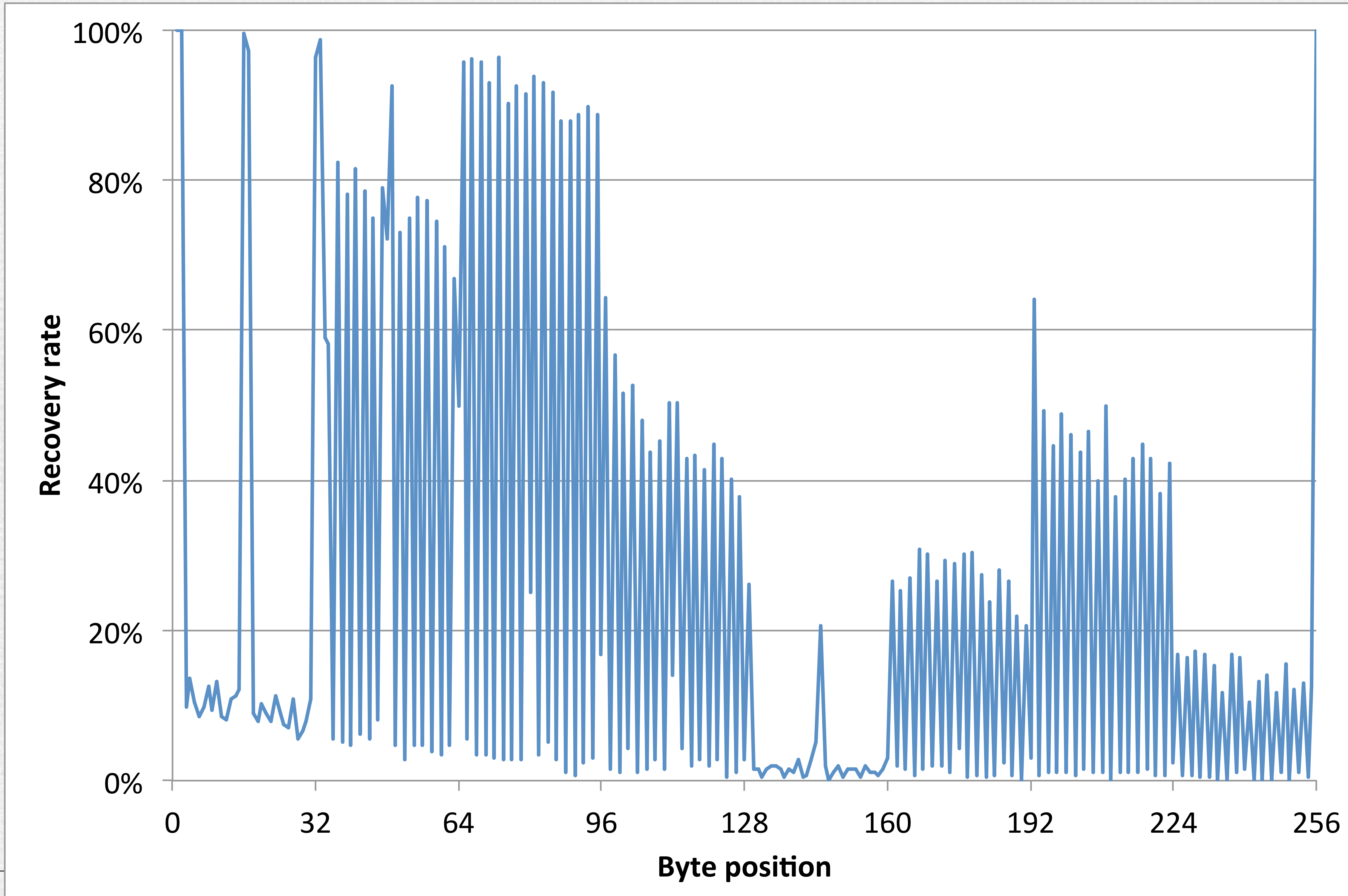


Color encoding: absolute strength of largest bias × 2^{16}

Plaintext Recovery Rate
2^{20} Frames

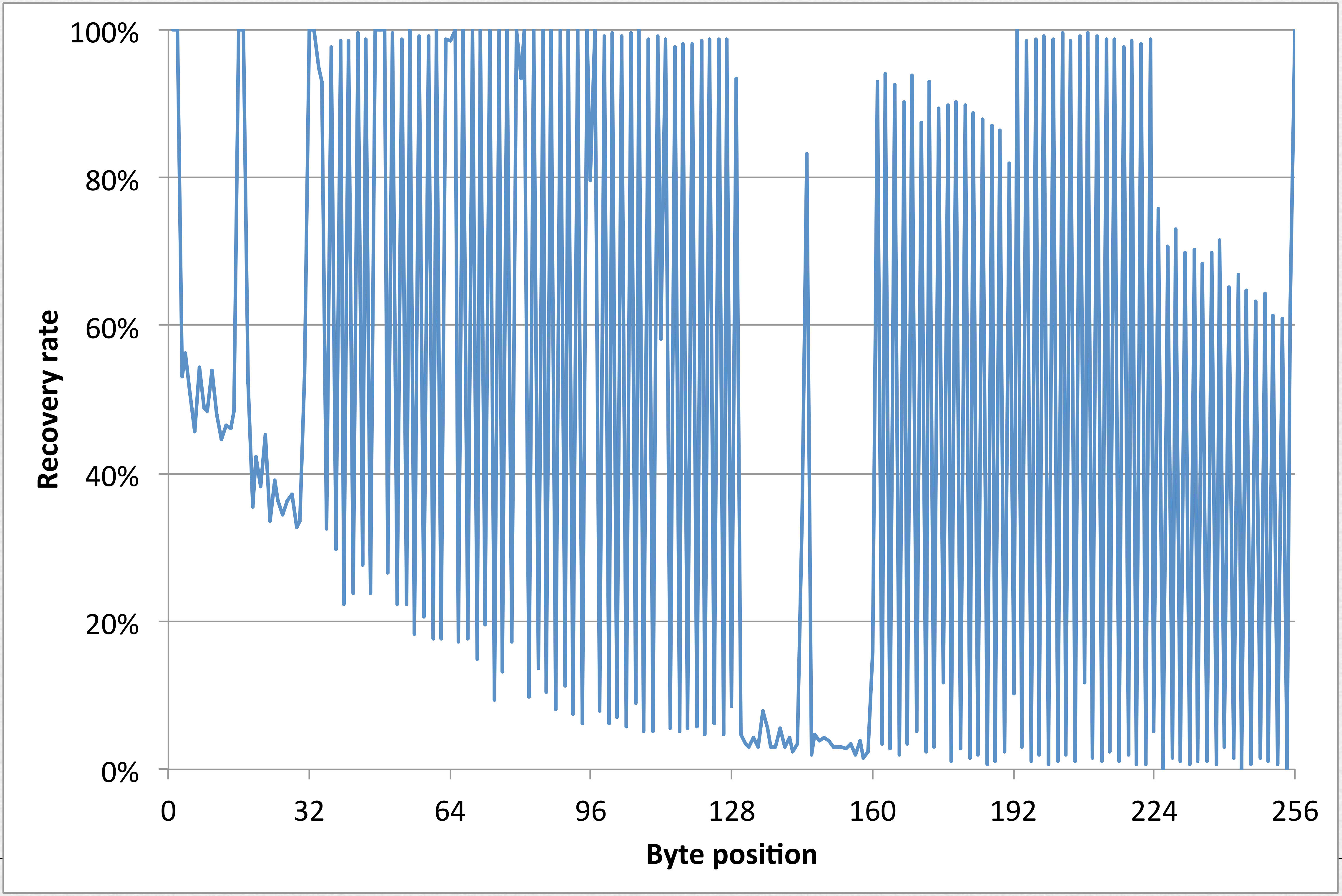


Plaintext Recovery Rate
2^{22} Frames



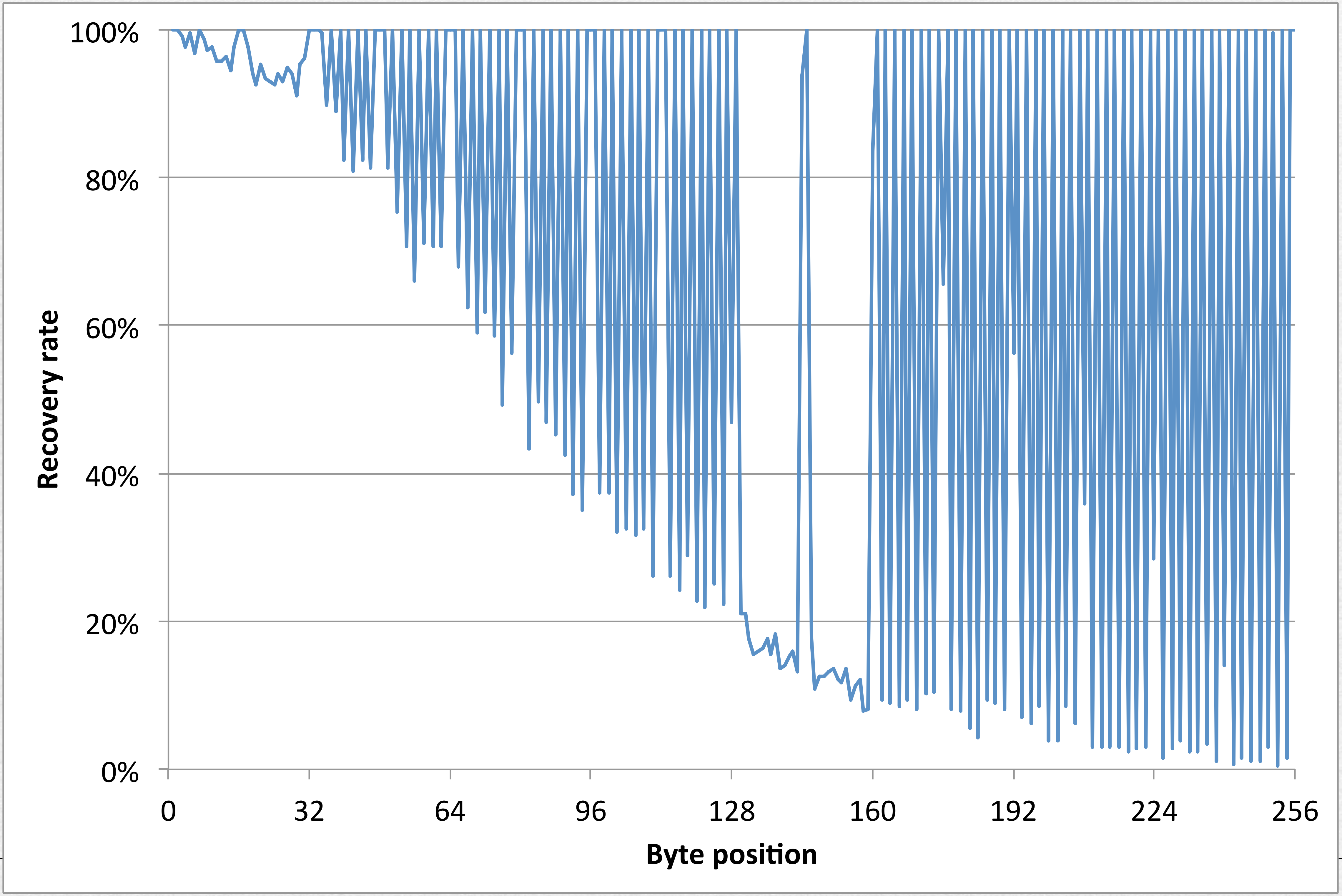
Plaintext Recovery Rate
2^{24} Frames

Information Security Group



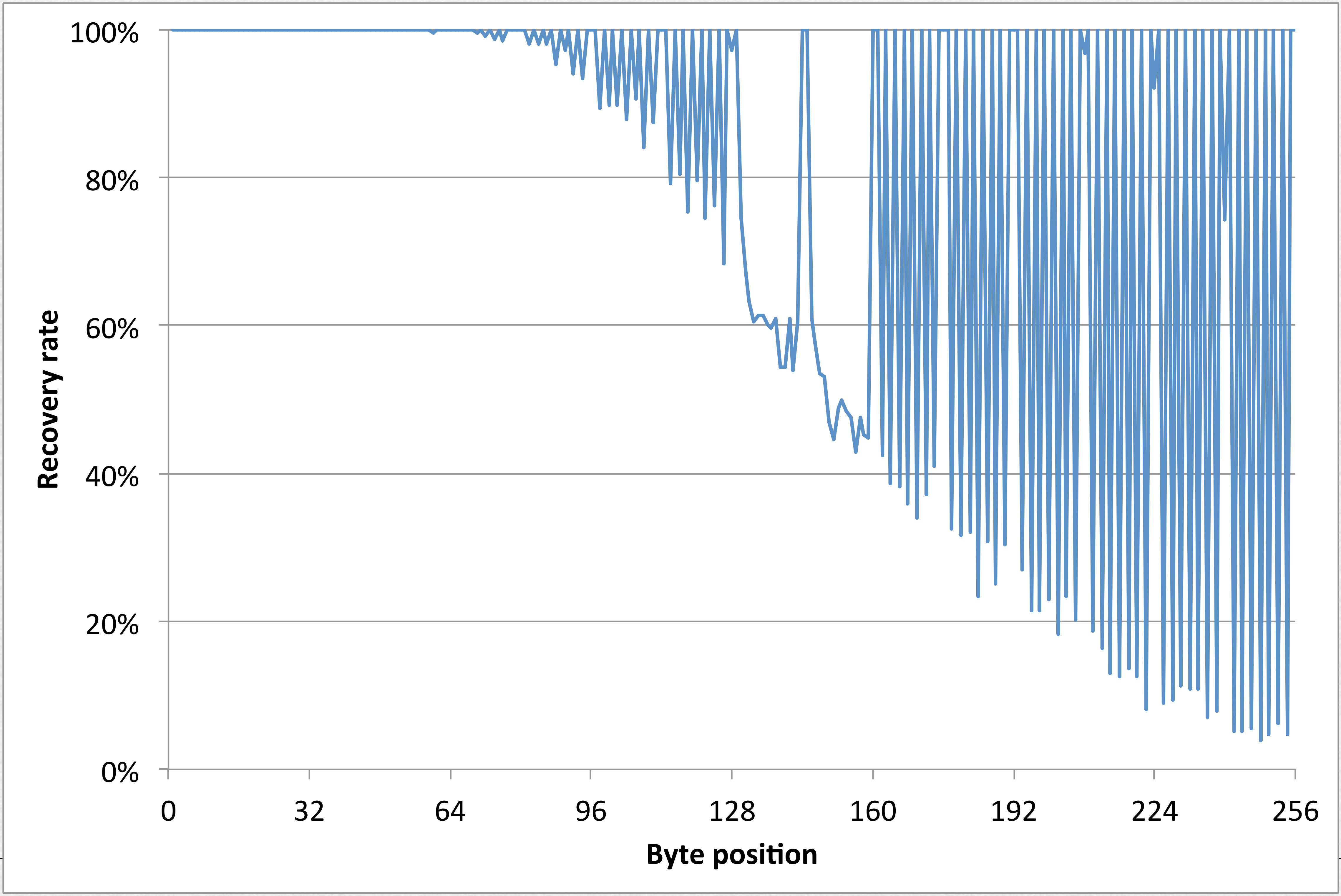
Plaintext Recovery Rate
2^{26} Frames

Information Security Group



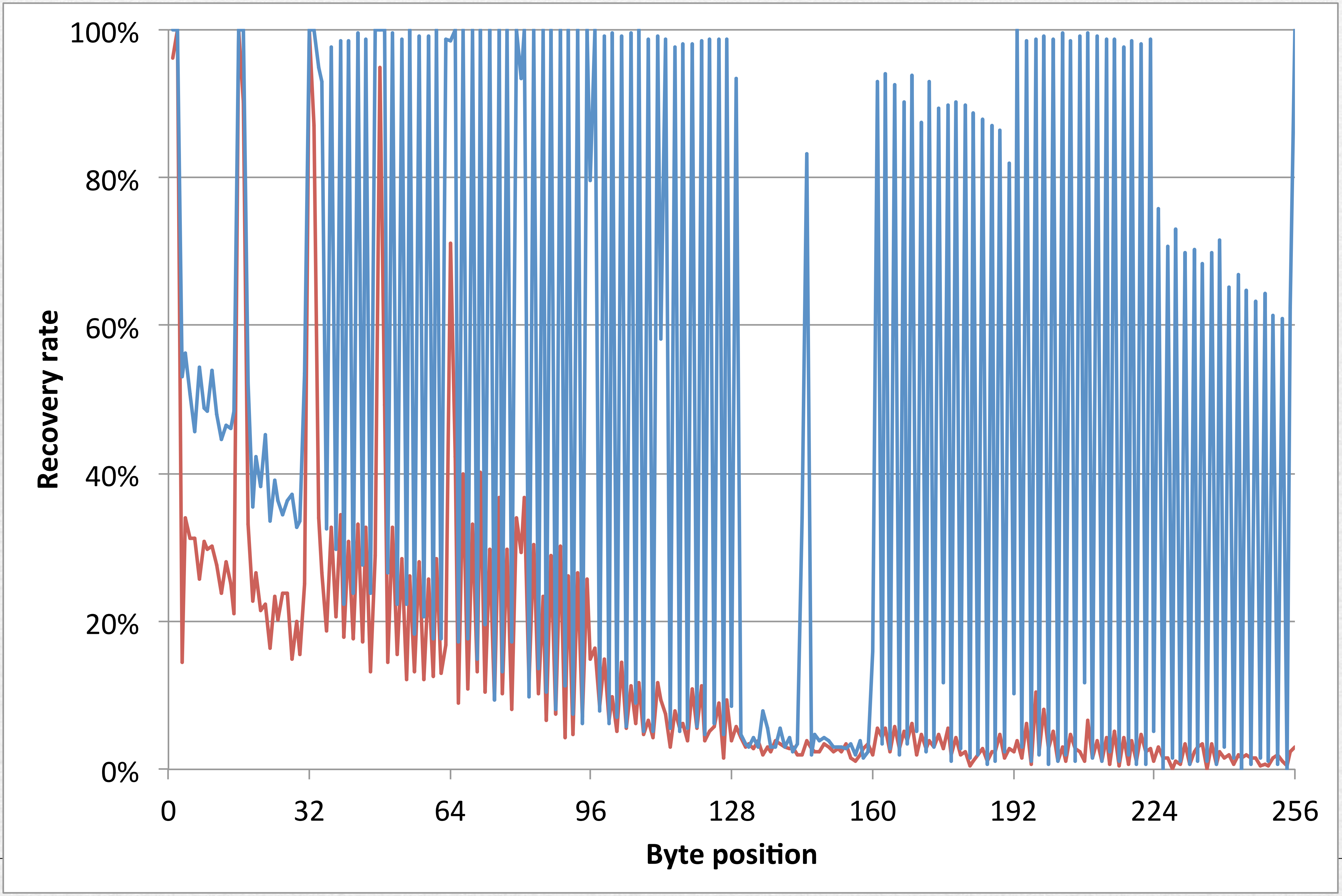
Plaintext Recovery Rate
2^{28} Frames

Information Security Group

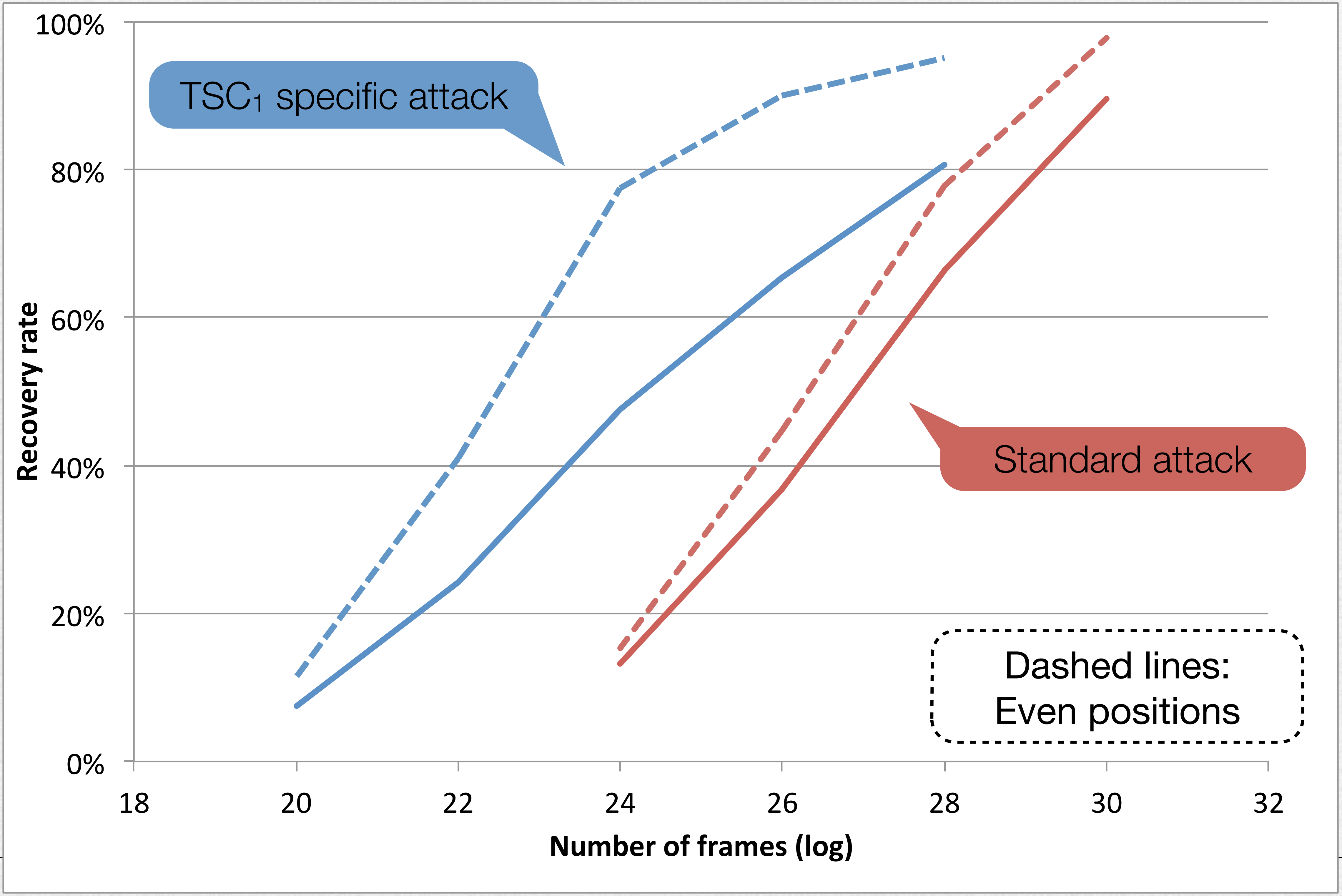


Comparison of Plaintext Recovery Rates 2^{24} Frames

Information Security Group



Comparison of Average Plaintext Recovery Rate



Concluding Remarks/Open Problems

Concluding Remarks

Information Security Group

- Plaintext recovery for WPA/TKIP is possible for the first 256 plaintext bytes, provided that sufficiently many independent encryptions of the same plaintext are available
- Security is far below the expected level of protection implied by the 128-bit key
- Suitable targets for attack might include fixed but unknown fields in encapsulated protocol headers or HTTP traffic via client-side Javascript
- Our attack complements known attacks on WPA/TKIP:
  - Passive rather than active (cf. Tews-Beck)
  - Ciphertext-only rather than known-plaintext (cf. Sepehrdad et al.)
  - Moderate amounts of ciphertext and computation
  - But requires repeated encryption of plaintext

Open Problems

Information Security Group

- Explain all the observed bias behaviour
  - Some progress has already been made by SenGupta-Maitra-Meier-Paul-Sarkar (next talk!)
  - Not essential for our plaintext recovery attack, but important for deeper understanding of RC4 in WPA/TKIP and for developing new attacks
- Carry out larger scale keystream bias computation over all (TSC_0,TSC_1) values and investigate how much improvement over our TSC_0-aggregated attack is possible
- Study other real-world applications of RC4 in which keys are changed frequently and/or have additional structure

Questions?