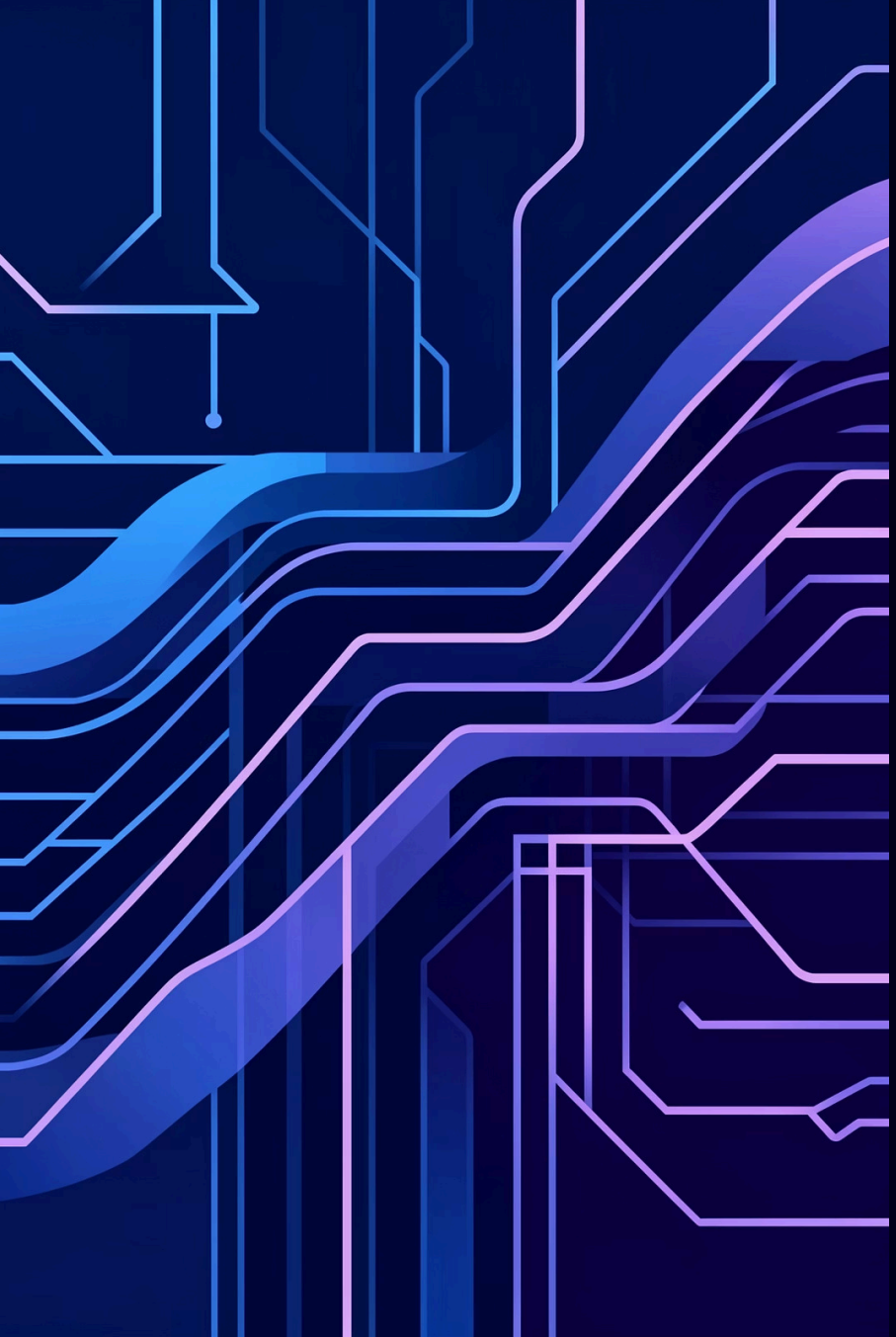
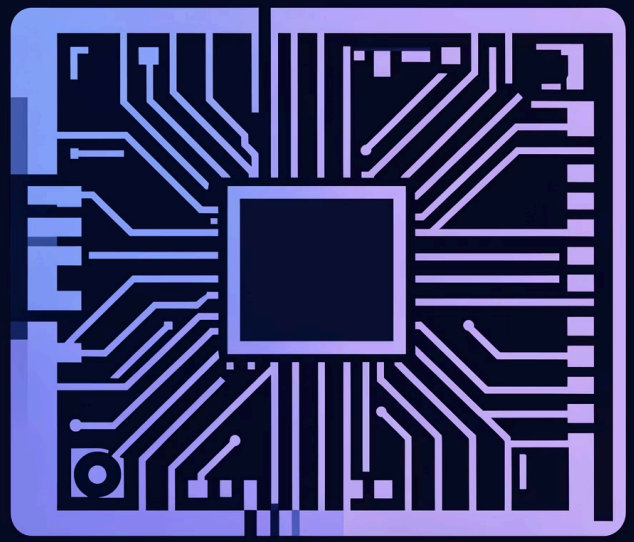


ZOSCII & Information Theory

Achieving perfect secrecy through zero overhead secure encoding on computers from the 1970s up to contemporary

2025

The Genesis of ZOSCII



Julian Cassin devised Zero Overhead Secure Code Information Interchange to dramatically increase text output performance on 8-bit computers. The breakthrough came when testing revealed something unexpected: the encoding achieved perfect security—a property thought impossible without sacrificing performance.

Before ZOSCII, 8-bit systems relied on ASCII or proprietary encodings like PETSCII, requiring expensive CPU operations for every character lookup.

The Traditional Character Lookup Problem

01

Table Base Address

Most 8-bit computers store ASCII tables in memory with a base address (DT) pointing to the character data table.

02

Calculate Offset

To retrieve character data (CD), calculate: CD = DT + AC × CDS, where AC is the ASCII value (e.g., 65 for 'A') and CDS is character data size.

03

Performance Cost

This multiplication operation is extremely expensive for 8-bit CPUs lacking multiplication instructions, requiring software emulation for every single character.

The Performance Breakthrough

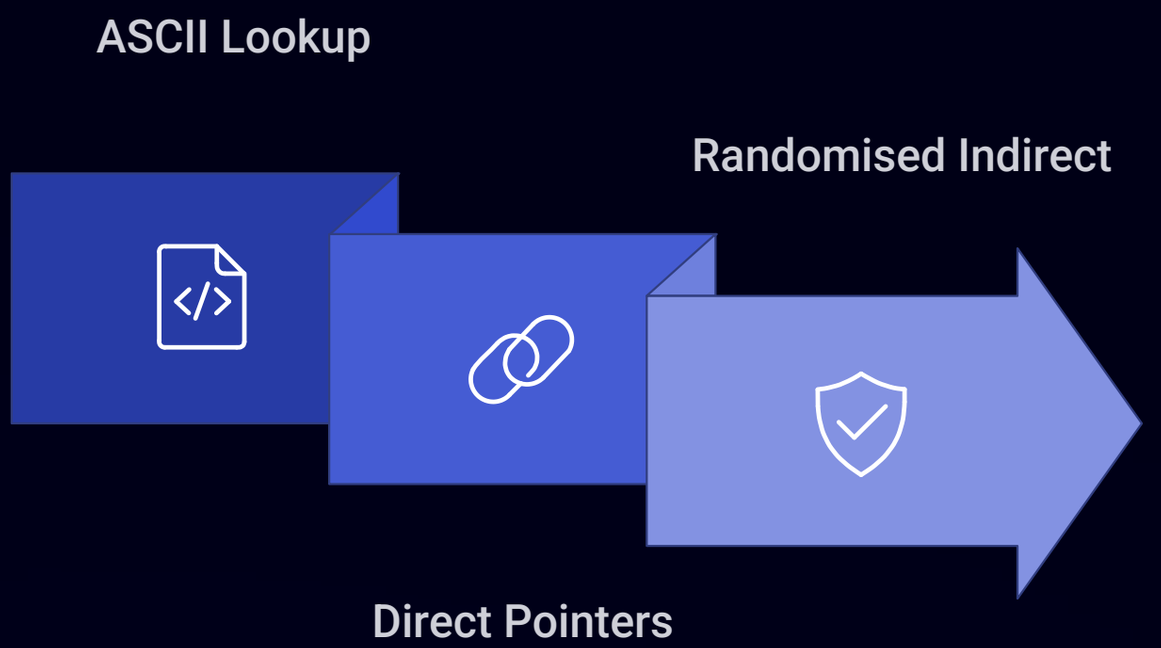
Direct Pointer Method

Replace expensive calculations with direct pointers to character data—achieving greater than 2× performance gain for text output operations.

Rather than using ASCII tables requiring multiplication, ZOSCII uses direct pointers to each character's data. This creates what's effectively a sprite or software sprite, eliminating the costly lookup calculation entirely.

But the real innovation comes from adding strategic indirection that transforms performance optimisation into perfect security.

From Performance to Perfect Security



Instead of storing direct character data references, ZOSCII adds indirection: point to a character value, read it, then look up the sprite table. The key insight? Within a 64KB memory map, there are hundreds of instances of each character value. Randomising which instance to use creates perfect security whilst maintaining maximum performance.

Requirements for Perfect Security

Sufficient Entropy

Each character must have multiple instances within ROM. A minimum of 5+ values per character provides adequate entropy with good random selection for perfect security.

Random Selection

Character instances must be chosen randomly at encoding time. High entropy allows "random enough" selection; low entropy requires perfectly balanced randomness.

Information Theory

This security model falls under Information Theoretic Security, as defined in Shannon's seminal 1949 paper *A Mathematical Theory of Communication*.

ZOSCII vs Traditional Security Methods

One-Time Pad

Achieves perfect security through XOR operations but requires key material as long as the message. Practical limitations make it unsuitable for most applications despite theoretical perfection.

Book Cipher

Traditional (page, paragraph, word references) use of a Book Cipher is considered not perfect security, but when using random ordinal character positions achieves perfect security but is impractical without computers.

Modern Encryption

Current trend for securing data and communications. Practical with computers but transforms data through mathematical operations, requiring decryption—fundamentally slower than memory lookup.

Why ZOSCII Isn't Encryption

Fundamental Difference

ZOSCII uses random character positions for encoding any data type (text, binary) with files of the user's choice. Each encoded value ranges from 0–65,535 in 16-bit ZOSCII, covering the full 64KB range.

Decoding is a simple memory lookup—a fundamental computer operation. On a Z80, a single `ld a, (hl)` instruction decodes the value at address hl.

Not Encryption

Encryption requires decryption. Memory lookup is not decryption—it's how computers fundamentally work.

Maximum Speed

No security mechanism can decode faster than a memory lookup. ZOSCII achieves theoretical minimum decoding time.

The Layman's Proof by Counterexample

> "I have five numbers in my head (the ROM), I won't tell you what it is, it's a secret—I will give you 5 pointers: #1, #2, #3, #3, #4. I guarantee given infinite time and compute you will NEVER guess it."

1

Unknown ROM

From an attacker's perspective, the ROM is random and unknown—providing no information about the message.

2

Plausible Deniability

Pointers like 1, 2, 3, 3, 4 could represent values 1 1 1 1 1, or 1 2 3 3 4, or 9 9 9 9 9—over 4 billion combinations with no way to determine the actual values.

3

Zero Information

Mathematical proof: I(M;A)=0. Random pointers to random ROM values equal zero information about the message.

Quantum-Proof Security Today

Shannon's Theorem

Entropy as measure of information and mutual information between source and destination form the mathematical foundation.

Perfect Secrecy

Zero mutual information via maximum uncertainty. All cryptanalytic attacks fail against weaponised ambiguity.

Future-Proof

Quantum computers cannot break Information Theoretic Security—ZOSCII provides quantum-proof protection today.

Further Reading

- Shannon's *A Mathematical Theory of Communication (1949)*
- One-Time Pad on Wikipedia
- ZOSCII Mathematical Proof
- ZOSCII Security Mathematical Proofs