

When Security & Hardware Meet: Key Concepts and Applications

Exploring encryption, authentication, and
hardware security solutions

Meeting Program

- Encryption Fundamentals
- Challenges in Key Management
- Trusted Platform Module (TPM)
- Hashing Techniques
- HMAC and Authentication Mechanisms
- Counterfeit Consumables in Medical Devices
- Cryptographic Solutions to Counterfeiting

Encryption Fundamentals

Definition and Purpose of Encryption



Encryption Categories

Encryption is divided into symmetric and asymmetric types, each with distinct methods and uses.

Purpose of Encryption

Encryption converts readable plain text into unreadable ciphertext to protect data privacy and security.

Secret Key Role

A secret key is essential to decrypt ciphertext back into readable plain text, ensuring secure communication.



Applications of Encryption

Access Control and Privacy

Encryption ensures that information can only be accessed by authorized individuals or systems, protecting privacy and security.

Data Integrity

Encryption helps verify that information has not been altered, ensuring data integrity during transmission or storage.

Challenges in Key Management

The 'Who Shaves the Barber?' Problem

Paradox Explanation

The 'Who Shaves the Barber?' is a logical paradox illustrating self-reference problems.

Plain Text vs Cipher Text

Plain text is readable by everyone, but cipher text requires a secret key for decryption.

Challenge of Secret Key

The main question is how to securely hide the secret key for encrypted data.



Limitations of Key Encryption

Recursive Key Encryption

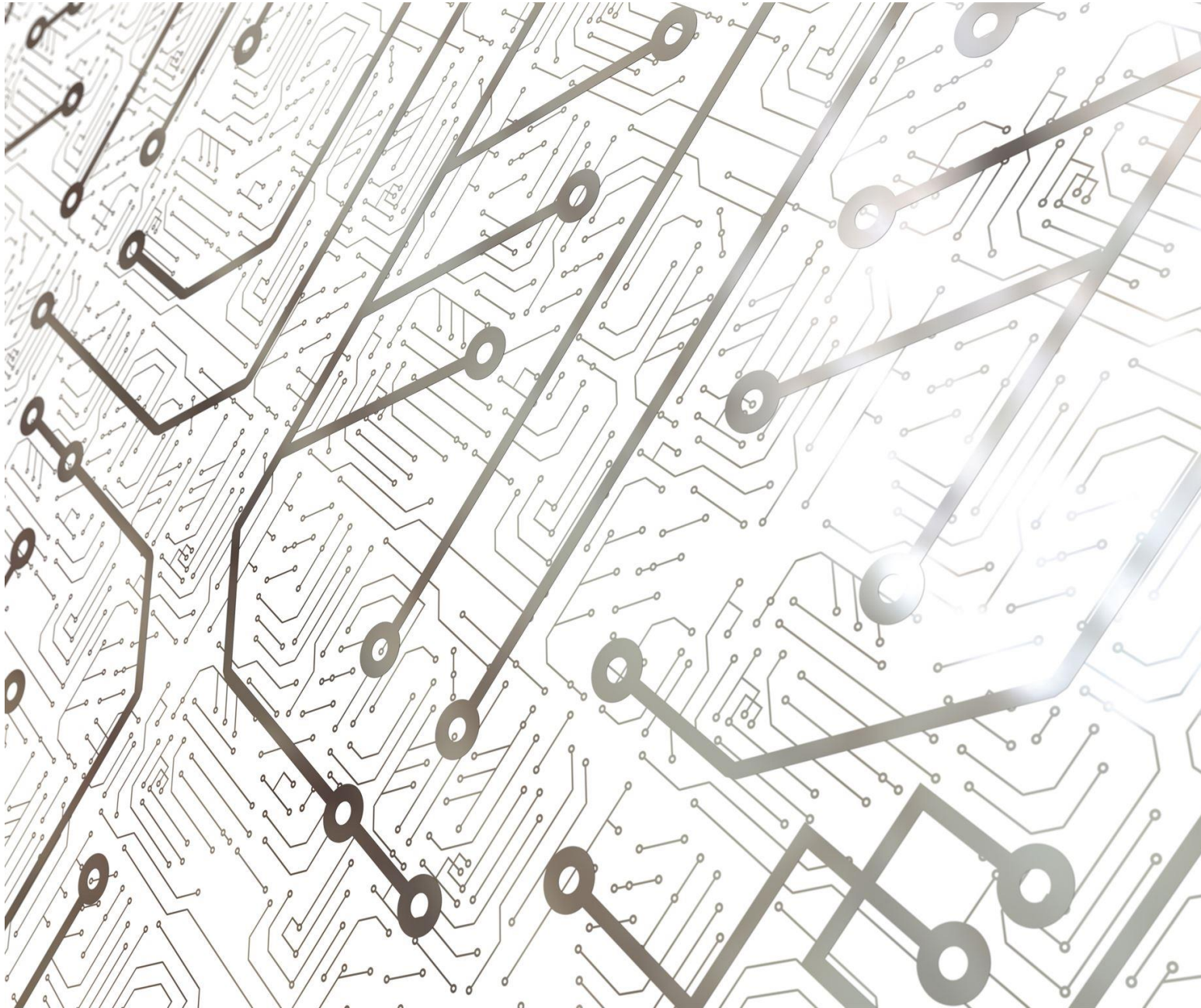
Encrypting data with multiple layers of keys can create a complex but not necessarily more secure system because we still do not know good way to hide “master” key

Exposure of Key Encrypting Keys

Even when keys are encrypted by other keys, the system remains vulnerable if key encrypting keys are exposed.



Trusted Platform Module (TPM)



Overview and Functions of TPM

Definition of TPM

TPM stands for Trusted Platform Module, a hardware security component embedded in devices to enhance protection.

TPM 2.0 Standard

The current TPM standard is version 2.0, which offers improved cryptographic capabilities and flexible security functions.

Core TPM Functions

TPM provides secure key storage, device authentication, and platform integrity checking to protect data.



Security Assurance Provided by TPM

Secure Secret Storage

TPM stores secrets in a secure hardware environment preventing unauthorized copying or extraction.

Built-in Cryptographic Operations

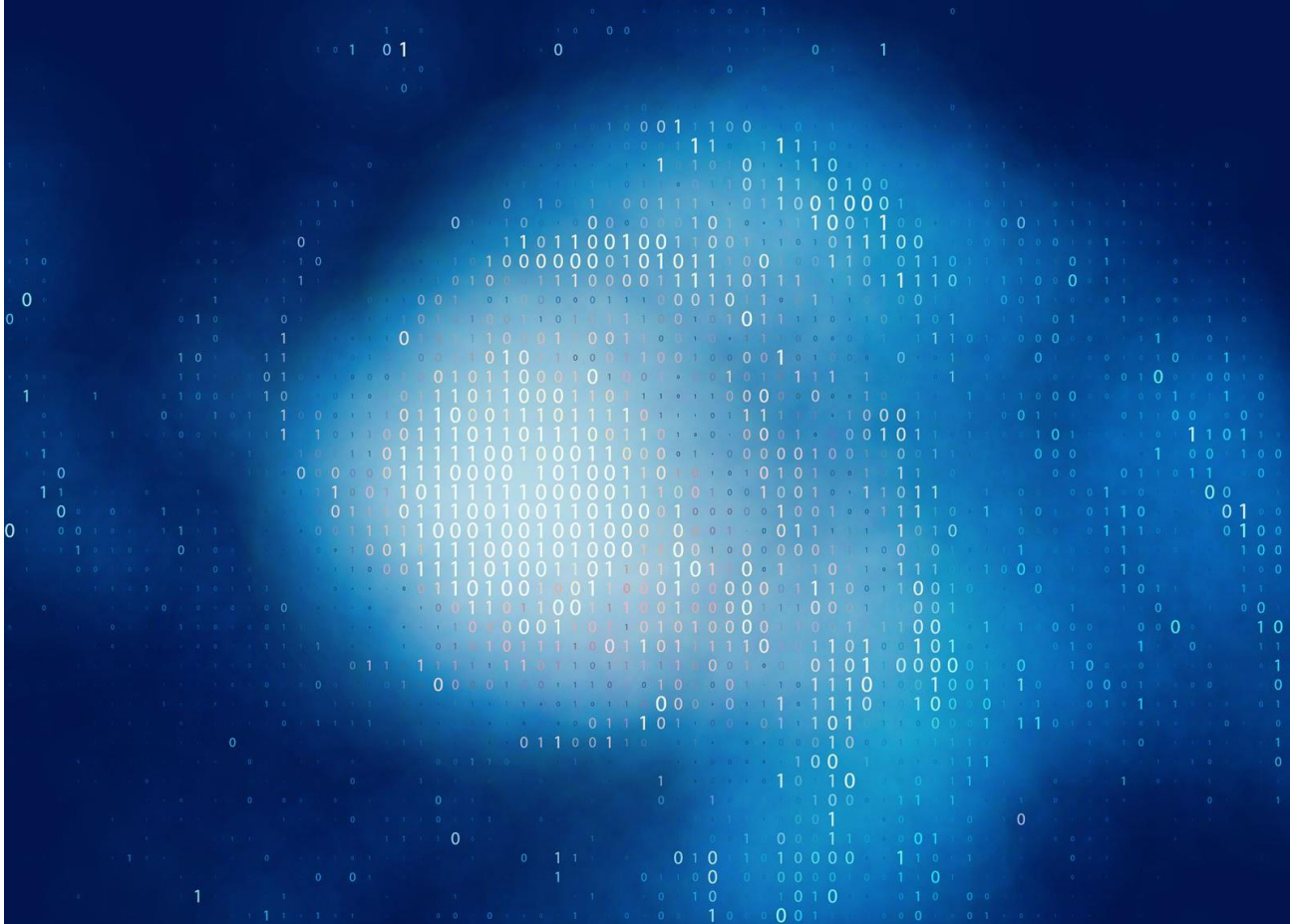
TPM performs encryption and decryption internally, ensuring sensitive keys never leave the module.

Protection Against Extraction

TPM ensures secrets cannot be extracted via logical or physical attacks, guaranteeing data integrity.

Hashing Techniques

Concept and Function of Hashing



Definition of Hashing

Hashing transforms input of any size into a fixed-size unique string representing the original data.

Purpose of Hashing

Hashing acts like a digital fingerprint, uniquely identifying data for security and integrity.

Common Hash Output and Uses



Hash Output Length

Common hash output strings are typically 256 bits long, ensuring strong cryptographic security.

Integrity Assurance

Hashing verifies data integrity by detecting any changes to the original information.

Authentication Usage

Hashes are widely used for authentication to confirm the identity of users and data sources.

HMAC and Authentication Mechanisms

Introduction to HMAC

Hashing Concept

HMAC builds upon hashing to enhance security by adding a secret into the hashing equation.

Use of Secret Keys

HMAC uses secret keys to authenticate messages, ensuring data integrity and authenticity.

Application in TPM

HMAC can be used with Trusted Platform Modules to provide hardware-based protection for secret stored



HMAC Process and Output

Input Concatenation

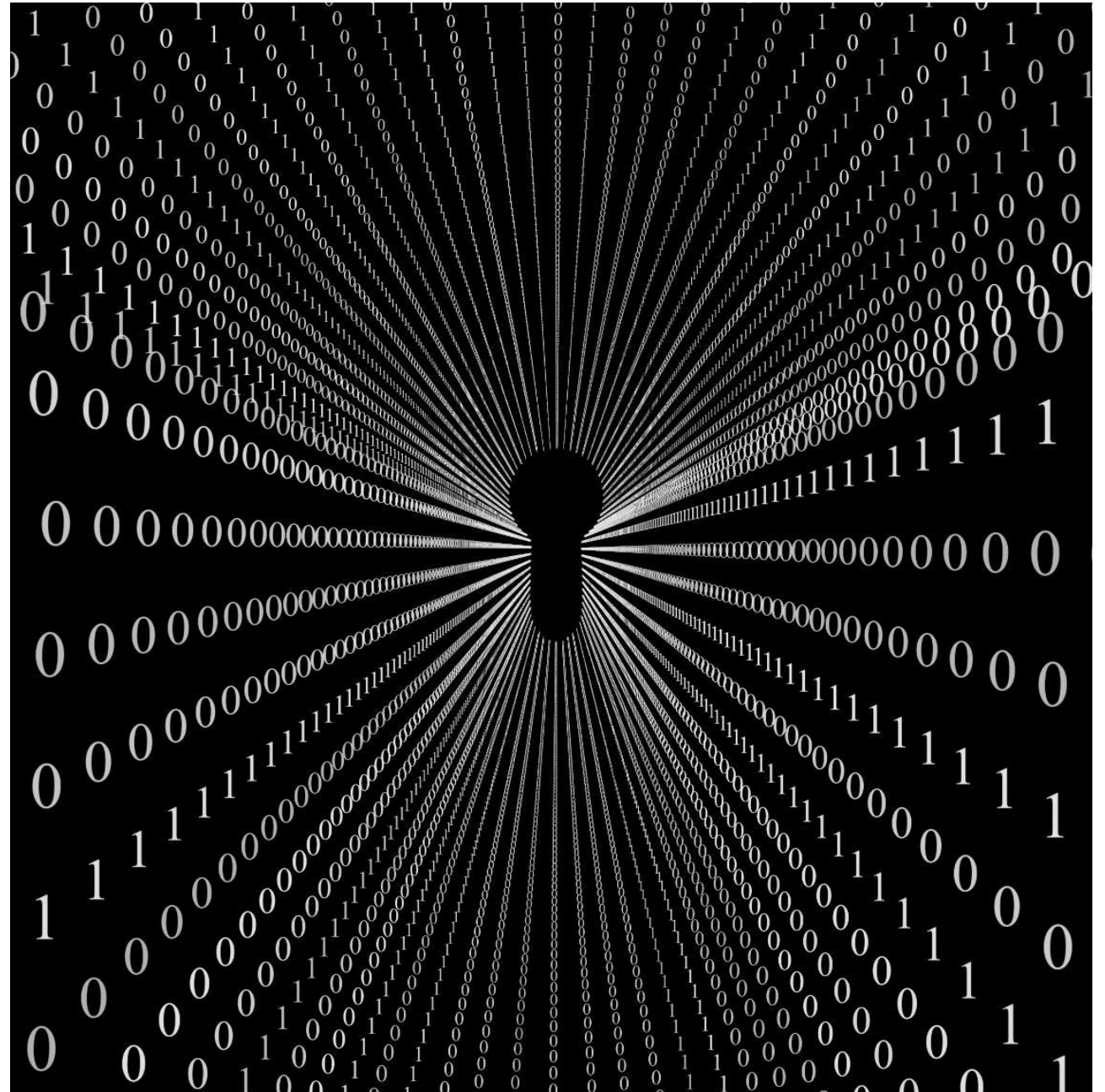
A data string is combined with a secret key stored securely in hardware modules like TPM before hashing.

Hashing Function

The concatenated string is processed through a cryptographic hashing algorithm.

HMAC Output

The final output is a 256-bit hash called the HMAC, used for secure authentication.



Counterfeit Consumables in Medical Devices



Revenue Distribution

Only 20% of revenue comes from selling the medical device itself.



Consumables Revenue

80% of revenue is generated from selling consumables required for device operation, ensuring continuous profit.



Business Model Strategy

The Razor & Blades model creates steady income through consumables after device purchase.



Impact and Prevalence of Counterfeit Consumables

Financial Loss to Manufacturers

Customers using counterfeit consumables causes manufacturers to lose up to 80% of their potential profit, impacting business sustainability.

Prevalence of Counterfeiting

Counterfeit consumables are widespread, with most medical device manufacturers encountering this challenge during operations at some point.

Need for Solutions

Manufacturers must develop effective strategies to detect and prevent counterfeit consumables to protect business and patient safety.

Cryptographic Solutions to Counterfeiting



Crypto Chips and HMAC Integration

Crypto Chips Overview

Crypto chips provide hardware-based security, similar to TPM but simpler, restricted to specific cryptographic functions.

Integration Mechanism

Crypto chips implement HMAC as one of the algorithms to securely authenticate consumable and verify data integrity in between consumable and device

Authentication Process Using Crypto Chips



Crypto Chips Pairing

Two identical crypto chips with matching secret keys are embedded on device and consumable for secure authentication.

Random String Exchange

Device generates a random string and sends it to the consumable to initiate the authentication process.

HMAC Generation

Consumable uses HMAC algorithm combining secret key and random string to generate a hashed message authentication code (HMAC) and sends this HMAC back to the device.

HMAC Verification

Device generates its own HMAC and compares it with consumable's HMAC to verify authenticity and allow usage.

Conclusion

Hardware Security Integration

Integrating security concepts with hardware solutions strengthens data protection and system integrity.

Counterfeit Prevention

Using crypto chips helps combat counterfeit consumables and ensures product authenticity.

Enhanced Trust and Safety

These technologies build trust by enhancing security and safety in critical applications.