IEEE CyberTrust workshop

Title: Deterministic random number generation for one time pads - Creating a Whitenoise super key

Author: André Brisson

Summary: A Whitenoise key is an exponential length key that can be used as a one-time-pad and that can in turn create an unlimited number of unique keys. Because its structure is more akin to the mechanical Enigma it is not vulnerable to arithmetic attacks. Because they are random they are resistant to brute force and quantum computing attacks.

IEEE

IEEE Computational Intelligence Society

One-time-pad network security

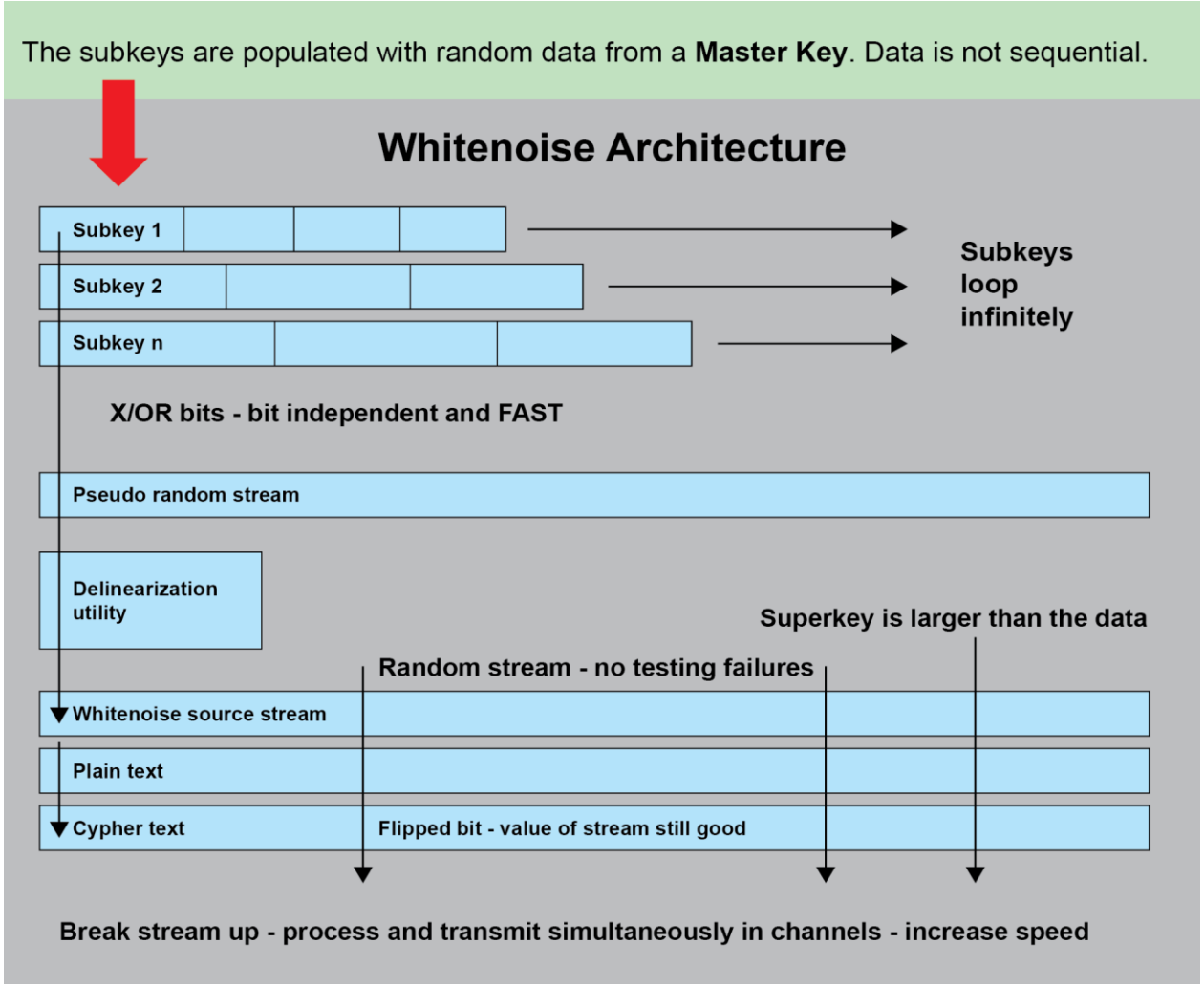
Whitenoise is a new generation stream cipher and deterministic random number generator.

Dynamic Identity Verification and Authentication **(DIVA)** is a virtual protocol exploiting Whitenoise keys (DRNG) as a one-time-pad.

Dynamic Distributed Key Infrastructures **(DDKI)** is a virtual security framework of devices and persons with DIVA. You can easily use it as a standalone distributed system or with existing asymmetric network frameworks to create a hybrid system that fixes PKI fatal flaws.

We will examine each in turn.

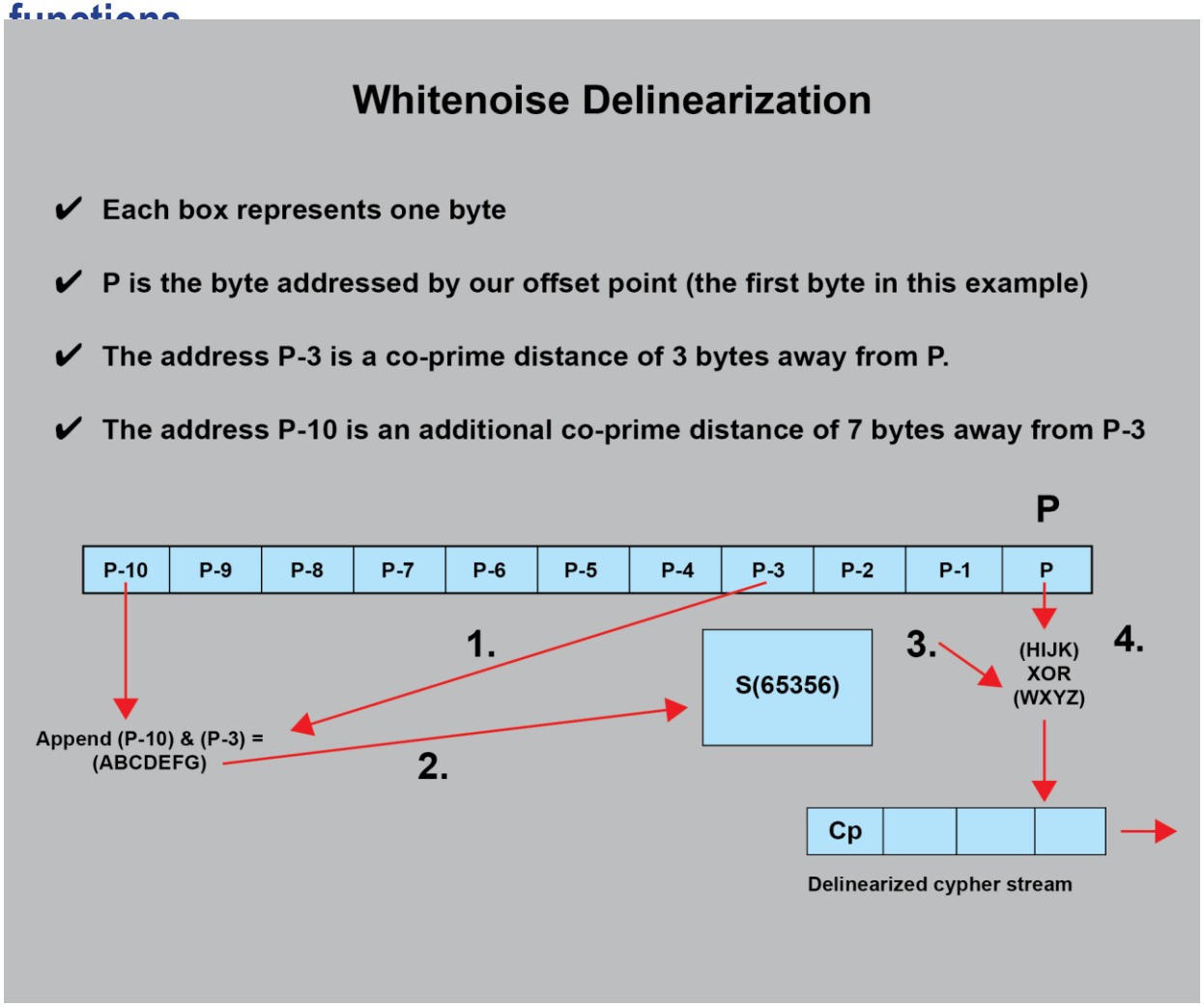
How a Whitenoise key (DRNG) is created



- Variable number of prime number length subkeys
- Each bit is XOr'd with the corresponding bit of the next subkey
- Two bytes worth are appended together and run through an S-box
- It becomes the first byte of the delinearized key stream

The subkeys loop infinitely left to right. We can use this data source only to the point where all the seams between all the subkeys line up perfectly vertically.

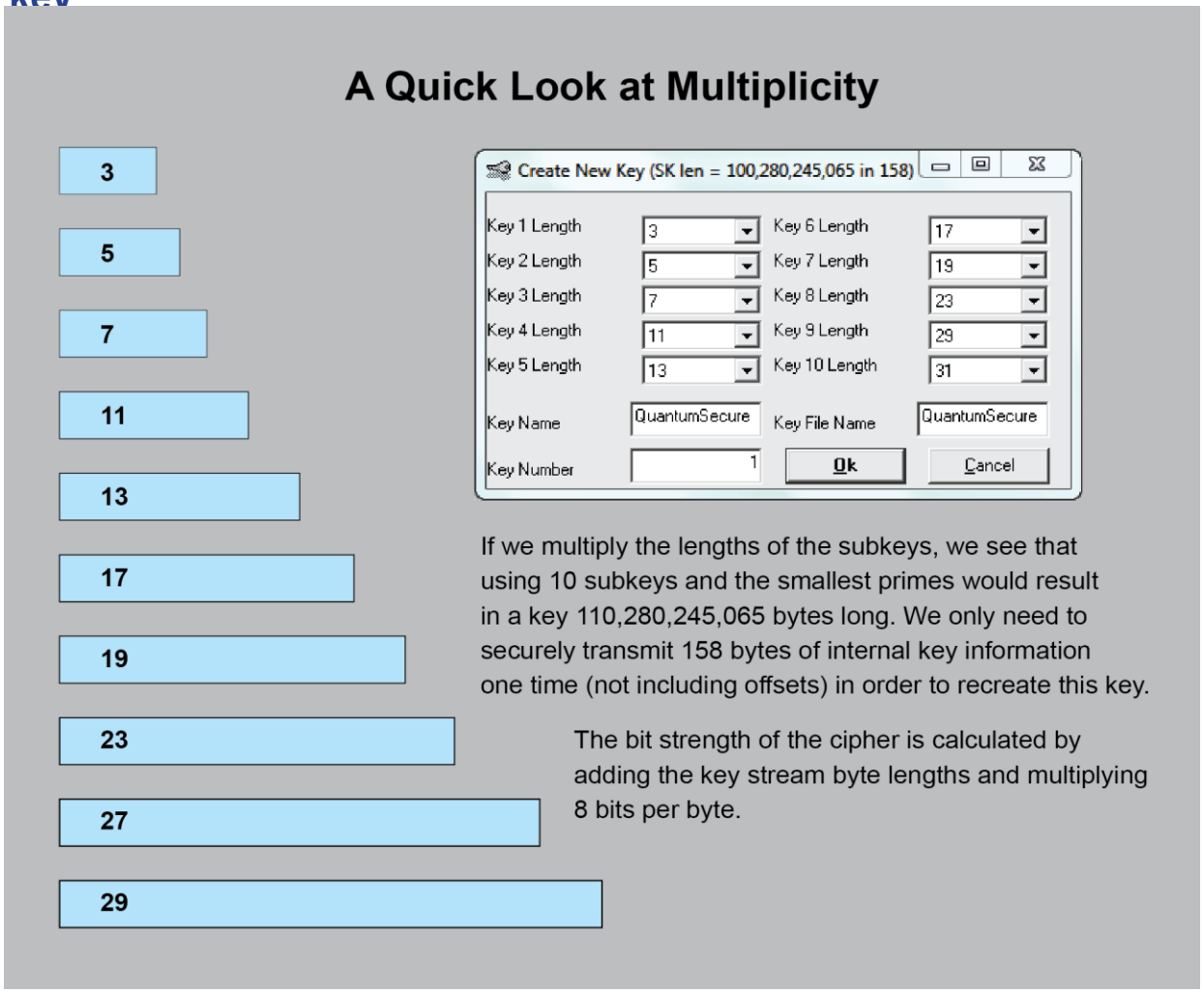
Whitenoise one-way functions



- Two bytes are taken from the initial key stream, appended together, and pushed through an S-Box
- Only one byte emerges
- A hacker cannot go backwards and guess two bytes of key stream from one byte of captured information
- The hacker has no knowledge of the number of subkeys, their lengths, or the random data they are populated with
- It is a one-time pad

The hacker has no knowledge of the master key which populates the subkeys with random data.

How to calculate length and strength of a Whitenoise key



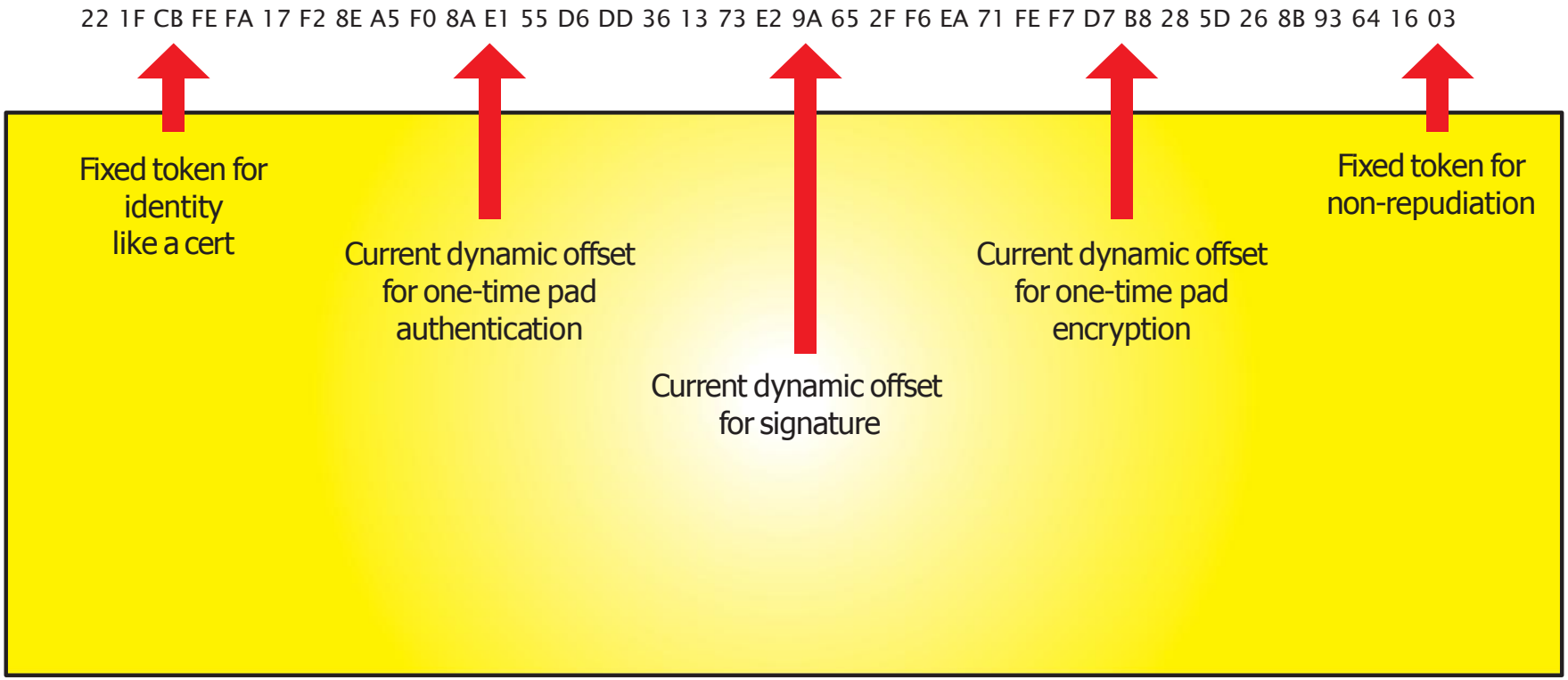
- The length of a Whitenoise key is calculated by multiplying the length of the subkeys in bytes
- The strength of a Whitenoise key is calculated by adding the lengths of the subkeys in bytes and multiplying by 8 bits per byte
- To create a key > 100 billion bytes long, we only have to store 158 bytes of information

This is the weakest key possible ~ 1600 bits. Bit strengths, key lengths, speed and entropy are easily scalable because Whitenoise is deterministic. Adding more subkeys results in greater entropy in the perturbed key.

Whitenoise key characteristics

- The key is an exponential **deterministic random number generator (DRNG)** data source.
- The government department, Telco or service provider receives a UNIQUE master key (DRNG).
- The entity can make an unlimited number of client account keys and distribute them to their customers or network endpoints **one time**.
- The unique, private, account keys create key streams of exponential length and are deterministic RNG themselves. Key structure storage requires little space.
- The unique, endpoint, distributed, private keys create an infinite number of unique one-time-pad tokens (small key subsets) from that one-time-distributed key.
- We know where each key-based cryptographic call or control is being called from in the key stream by tracking current dynamic offsets.
- Using keys is incredibly fast because after key setup the only function is XOr which is the fastest operation on a computer. This allows Whitenoise to be used in IoT and sensor contexts that cannot use cryptography with high overhead like RSA, ECC and AES.

Track all key based security controls from one infinite deterministic random key stream



Key characteristics

- The keys and tokens can be of ANY bit strength.
- Smaller tokens for authentication can be safely used because DIVA operates as a dynamic, continuous, one-time pad.
- Because the keys are unique to each endpoint or device they provide authenticated encryption for storage or transmission with provenance and identity.
- Because keys use the fastest function available on computers, XOr, it is always as fast as the hardware.
- Because the keys are bit independent they can be parsed and cut up and reassembled. This ensures secure key storage separating key structure and offsets and scalable speed.
- In hardware (like FPGAs), **2 bytes per clock cycle** are processed. Speed is scalable by adding more threads. The fastest RSA algorithm (Spritz 2014) needs 24 clock cycles to process one byte. AES-NI needs 28 clock cycles per byte. Both Spritz and AES-NI are slow and computationally intensive. Whitenoise is side channel attack resistant .

Security Analysis — University of California, Berkeley

https://eprint.iacr.org/2003/218.pdf

David Wagner could find no effective mathematical attack. He also concluded:

"With the recommended parameters, Whitenoise uses keys with at least 1600 bits randomness. Exhaustive search of 1600 bit keys is completely and absolutely infeasible. Even if we hypothesized the existence of some magic computer that could test a **trillion-trillion** key trials per second (very unlikely!), and even if we could place a **trillion-trillion** of these computers somewhere throughout the universe (even more unlikely!), and even if we were to wait a **trillion-trillion** years (not a chance!), then the probability that we would discover the correct key would be negligible (about ½ to the 1340 power which is unimaginably small – $1/2^{1340}$). Hence, if keys are chosen appropriately and Whitenoise is implemented correctly, exhaustive key search is not a threat."

David Wagner
– University of California, Berkeley

Why Whitenoise is Quantum Computing Attack Resistant

- **Quantum computing attacks are prevented** because every variable is dynamic
- No attack is effective against a one time pad
- The quantum attacker has no knowledge of master key
- The quantum attacker has no knowledge of the number of subkeys, their lengths or the non-sequential random data that they are populated with
- The best chance of breaking Whitenoise is with brute force attacks, but the quantum attacker cannot go backwards and guess two bytes from one byte of capture information

DEMO

END