a sequential memory-hard key derivation function with better measurable security

caveman

January 1, 2021

Abstract

hi — i propose *ciphart*, a sequential memory-hard key derivation function that has a security gain that's measurable more objectively and more conveniently than anything in class known to date.

to nail this goal, *ciphart*'s security gain is measured in the unit of *relative entropy bits.* relative to what? relative to the encryption algorithm that's used later on. therefore, this *relative entropy bits* measure is guaranteed to be true when the encryption algorithm that's used with *ciphart* is also the same one that's used to encrypt the data afterwards.

1 intro

first i'll describe the ciphart algorithm, then i will tell you why it's memory hard, and how it offers better measurable security.

2 ciphart

input:

e	number of entropy bits to be added.
k	initial key.
f	encryption function.
m_i	memory pad.

output:

$\hat{k}$	better key.

steps:

```
define $p, t, r$ such that $ptr - 2^e$ is smallest positive number.
for $p = 0$ to $p = P$ do
    for $t = 0$ to $t = T$ do
        for $r = 0$ to $r = R$ do
            $n \leftarrow p \oplus t \oplus r$
        end for
    end for
end for
```