sequential memory-hard key derivation 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.

Contents

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:	b	number of entropy bits to be added.
	k	initial key.
	f	encryption function.
	m_i	memory pad, at least 32 bytes.
	R	number of rounds per task.
output:	$\hat{k}$	better key.

define P, T such that $PTR-2^b$ is smallest positive number, and that T is an even number.
for $p = 1$ to P **do**
  for $t = 1$ to T in steps of 2 **do**
    $a \leftarrow t$
    $b \leftarrow t + 1$
    for $r = 1$ to $2R$ **do**
      $n \leftarrow p^\frown t^\frown r$
      $m_a \leftarrow f(m_b, k, n)$
      $\hat{a} \leftarrow a$
      $a \leftarrow b$
      $b \leftarrow \hat{a}$
    end for
  end for
end for

3 sequential-memory hardness

4 better security interpretation