

# Layered Counter Chaining

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-10/1260.html>

---

**From:** John Savard ([jsavard\\_at\\_excxn.aNOSPAMb.cdn.invalid](mailto:jsavard_at_excxn.aNOSPAMb.cdn.invalid))

**Date:** 10/28/04

Date: Thu, 28 Oct 2004 07:42:46 GMT

On my web page, at

<http://home.ecn.ab.ca/~jsavard/crypto/co040603.htm>

I have now added a description, and a diagram, of a relatively simple encryption mode which aims to be almost all things to all men.

It is not parallelizable, though. The CBC-like chaining that prevents it from being parallelizable may be completely unnecessary.

I choose a random IV, and encrypt it twice.

The value after one encryption is used to seed a counter which is simply incremented once for each block.

The value before any encryptions starts an accumulator, which keeps having the counter value added to it.

Incrementing the counter doesn't change it much, so, if it weren't for carries – if the counter were XORed to the accumulator – accumulator values separated by an even number of blocks would be nearly identical.

Encrypting a block involves one block cipher operation. But the accumulator is XORed with the value before and after encryption.

And on top of that, the previous block cipher output is XORed with the value before encryption.

Since the counter is just a counter, and predictable if you know the key to recover the IV, the previous block output is available from any block without depending on the block output from the block before, so garbles only affect two blocks.

The counter seems to have the absolute minimum in complexity required to avoid the attacks used against the withdrawn integrity-aware mode from some NSA employees. Security against all forgeries requires at least using a checksum with the mode, of course. Also, it seems to offer the potential of increasing security just by using a different key for

## sci.crypt: Layered Counter Chaining

encrypting the IV; it's hard to see how a brute-force search could then attack either key separately.

But with only a one-block IV, it is vulnerable to birthday attacks that can obtain two messages enciphered with the same IV, unlike my attempts at an integrity-aware mode.

Still, I think I have come up with an "all-purpose" mode which, with a minimum of extra overhead, is hard to misuse. (Letting the submitter of plaintext pick his own IV, of course, would vitiate the extra features of the mode.)

John Savard

<http://home.ecn.ab.ca/~jsavard/index.html>