

## Re: Sinople: a 128-bit symmetric block cipher

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-03/1270.html>

---

**From:** Philippe Paquet ([ppaquet@reflectionsinteractive.com](mailto:ppaquet@reflectionsinteractive.com))

**Date:** 03/10/03

From: "Philippe Paquet" <[ppaquet@reflectionsinteractive.com](mailto:ppaquet@reflectionsinteractive.com)>

Date: Mon, 10 Mar 2003 21:14:31 GMT

BEAR and LION are really different. They use hash function and a stream cipher in their construction. ref:

– Two Practical and Provably Secure Block Ciphers: BEAR and LION (Ross Anderson, Eli Biham)

– A Critique of BEAR and LION (Pat Morin)

"David Wagner" <[daw@mozart.cs.berkeley.edu](mailto:daw@mozart.cs.berkeley.edu)> wrote in message news:b4gfpb\$20jh\$1@agate.berkeley.edu...

> *Martin4* wrote:

> >Are there other UFNs which combine source-heavy and target-heavy

> >rounds in this manner?

>

> *BEAR and LION* come to mind.