NAME

padlock - driver for the cryptographic functions and RNG in VIA C3, C7 and Eden processors

SYNOPSIS

To compile this driver into the kernel, place the following lines in your kernel configuration file:

```
device crypto
device padlock
```

Alternatively, to load the driver as a module at boot time, place the following line in loader.conf(5):

```
padlock_load="YES"
```

DESCRIPTION

The C3 and Eden processor series from VIA include hardware acceleration for AES. The C7 series includes hardware acceleration for AES, SHA1, SHA256 and RSA. All of the above processor series include a hardware random number generator.

The **padlock** driver registers itself to accelerate AES operations and, if available, HMAC/SHA1 and HMAC/SHA256 for crypto(4). It also registers itself to accelerate other HMAC algorithms, although there is no hardware acceleration for those algorithms. This is only needed so **padlock** can work with ipsec(4).

The hardware random number generator supplies data for the kernel random(4) subsystem.

SEE ALSO

crypt(3), crypto(4), intro(4), ipsec(4), random(4), crypto(7), crypto(9)

HISTORY

The **padlock** driver first appeared in OpenBSD. The first FreeBSD release to include it was FreeBSD 6.0.

AUTHORS

The **padlock** driver with AES encryption support was written by Jason Wright <*jason@OpenBSD.org*>. It was ported to FreeBSD and then extended to support SHA1 and SHA256 by Pawel Jakub Dawidek <*pjd@FreeBSD.org*>. This manual page was written by Christian Brueffer <*brueffer@FreeBSD.org*>.