NAME

armv8crypto - driver for the AES accelerator on ARM CPUs

SYNOPSIS

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

```
device crypto
device armv8crypto
```

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

```
armv8crypto_load="YES"
```

DESCRIPTION

Starting with the ARMv8 architecture ARM Limited has added optional cryptography instructions to accelerate AES, SHA-1, SHA-2, and finite field arithmetic.

The processor capability is reported as AES in the Instruction Set Attributes 0 line at boot. The **armv8crypto** driver does not attach on systems that lack the required CPU capability.

The **armv8crypto** driver registers itself to accelerate AES operations for crypto(4).

SEE ALSO

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

HISTORY

The **armv8crypto** driver first appeared in FreeBSD 11.0.

AUTHORS

The **armv8crypto** driver was written by Andrew Turner <*andrew@FreeBSD.org*>.