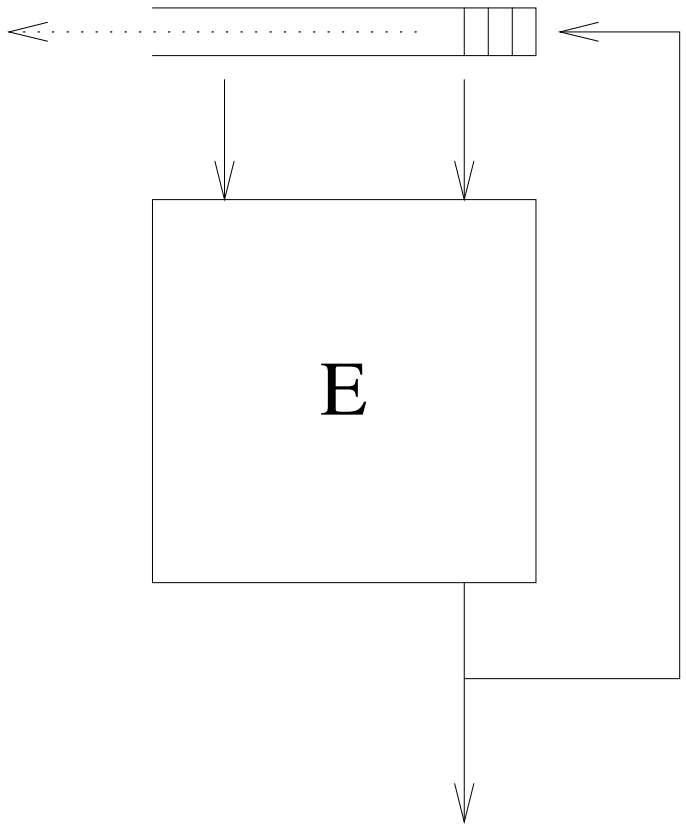
New weaknesses in t-bit OFB and CFB modes

(for small t)

David Wagner

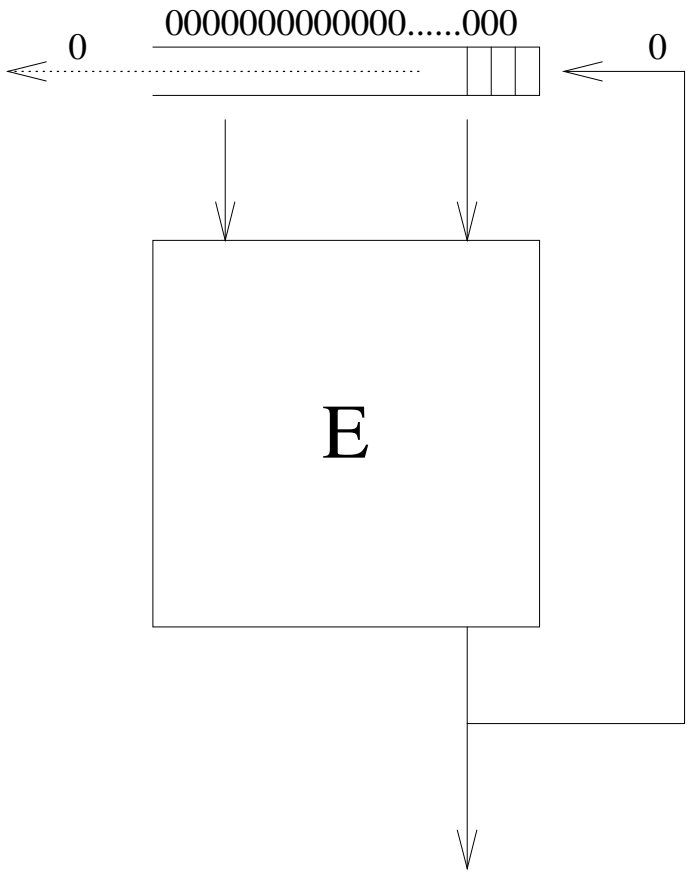
University of California, Berkeley

1-bit OFB mode



For simplicity, we'll focus on 1-bit OFB mode; the properties also generalize (with increased complexities) to the t-bit modes, for small t.

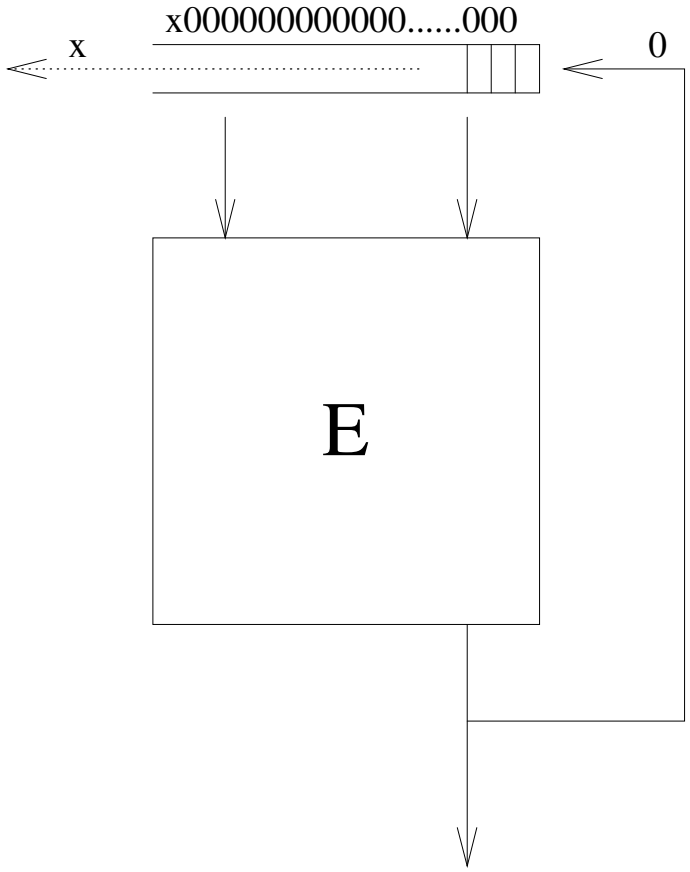
Short cycles



If $E(00\ldots0) = 0$ (probability 1/2), then IV=$00\ldots0$ gives all-zeros keystream output, forever.

(Generalizes to any periodic IV, with decreased success probability.)

Differential weaknesses



Let $\Delta = 10000\ldots0$.

If $E(IV) = E(IV \oplus \Delta)$ (probability 1/2), then both IV and $IV \oplus \Delta$ give the same keystream output, forever.

And...

Using a counter as your IV with t-bit OFB (or CFB) mode can be very dangerous.