Cryptanalysis of some recently-proposed multiple modes of operation

David Wagner
University of California, Berkeley
daw@cs.berkeley.edu

Organization

- Multiple modes as mini-protocols.
- Some chosen-IV attacks on multiple modes:
  - Divide-and-conquer attacks
  - Narrow-pipe attacks
- Countermeasures: more sophisticated protocols, and their failure modes.

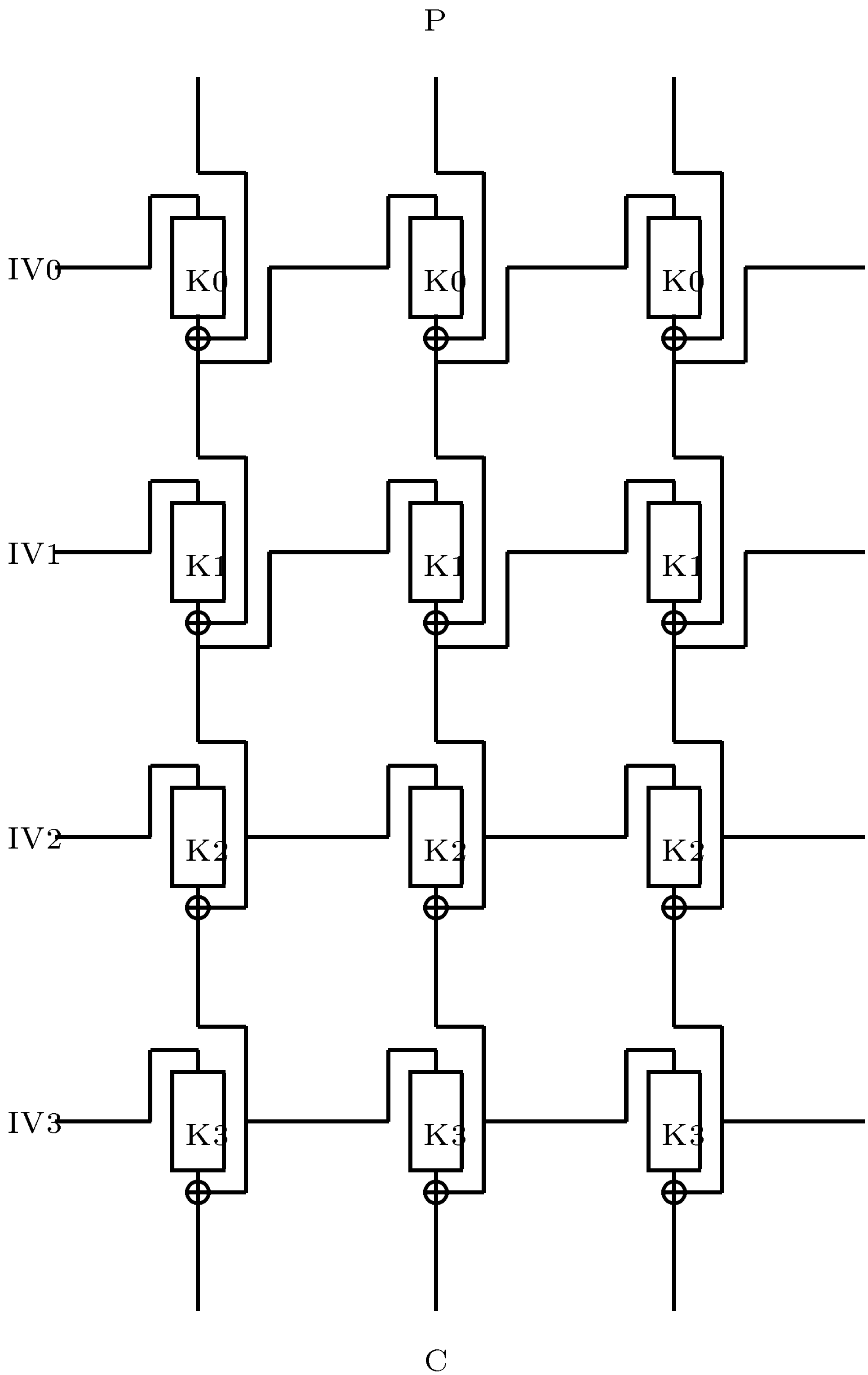
Some multiple modes

Notation [Biham]:

- $M \mid N$: output of mode M fed to input of mode N.
- OFB[M]: $\text{OFB}_{K0} \mid M \mid \text{OFB}_{K0}$.
- $M \to N$: keystream from stream mode M fed to input of mode N; resulting output is xor-ed against the plaintext.
- Independent keying for each mode.
- Independent IVs for each mode.

Biham recently proposed 4 triple modes and 5 quad modes of this form.

An example



The CFB|CFB|CFB^{-1} |CFB^{-1} mode.

Mini-protocols

Can view a multiple mode as a mini-protocol:

$$1. \quad A \rightarrow B: \quad IV0, \ldots, IVn, C$$

where C is a ciphertext for the multiple mode.

With this view, we see an asymmetry:

> Chosen-ciphertext attacks on the protocol are more powerful than chosen-plaintext attacks, because the former allow the attacker to choose the IVs.

Therefore, we propose to analyze the security of multiple modes against chosen-ciphertext chosen-IV attacks.

Divide-and-conquer attacks

Cryptanalysis of CFB|CFB|CFB^{-1} |CFB^{-1}.

Isolate $K0$:

1. Force a Δ into $IV0$:
   - Choose two ciphertexts differing only in $IV0$.
   - Get their decryption.
2. We get the relation

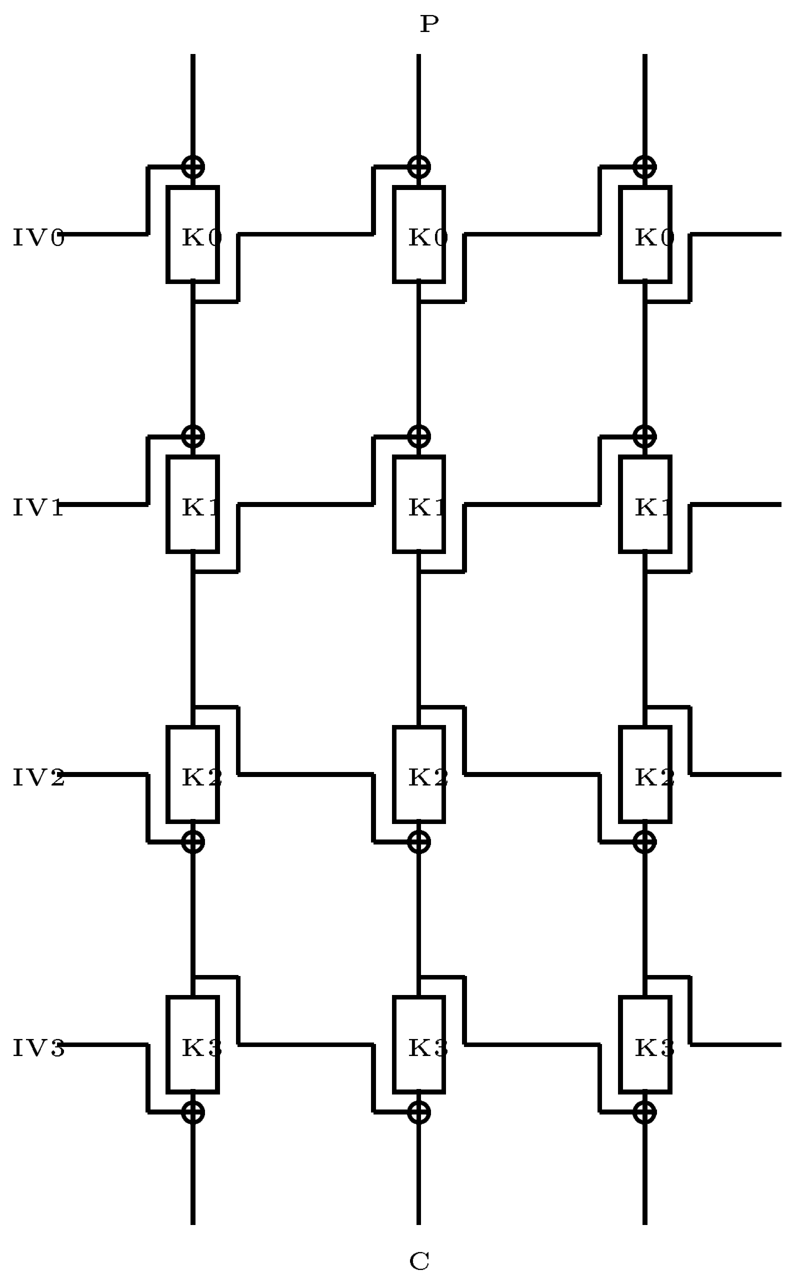
$$P_0 \oplus P_0' = E_{K0}(IV0) \oplus E_{K0}(IV0').$$

3. Find $K0$ by exhaustive keysearch.

Continue, recovering Ki by probing IVi.
Complexity: 3 chosen-IV chosen-ciphertexts, $7 \cdot 2^{56}$ work.

Another example

Divide-and-conquer fails: shoving a Δ into $IV2$ doesn't work.

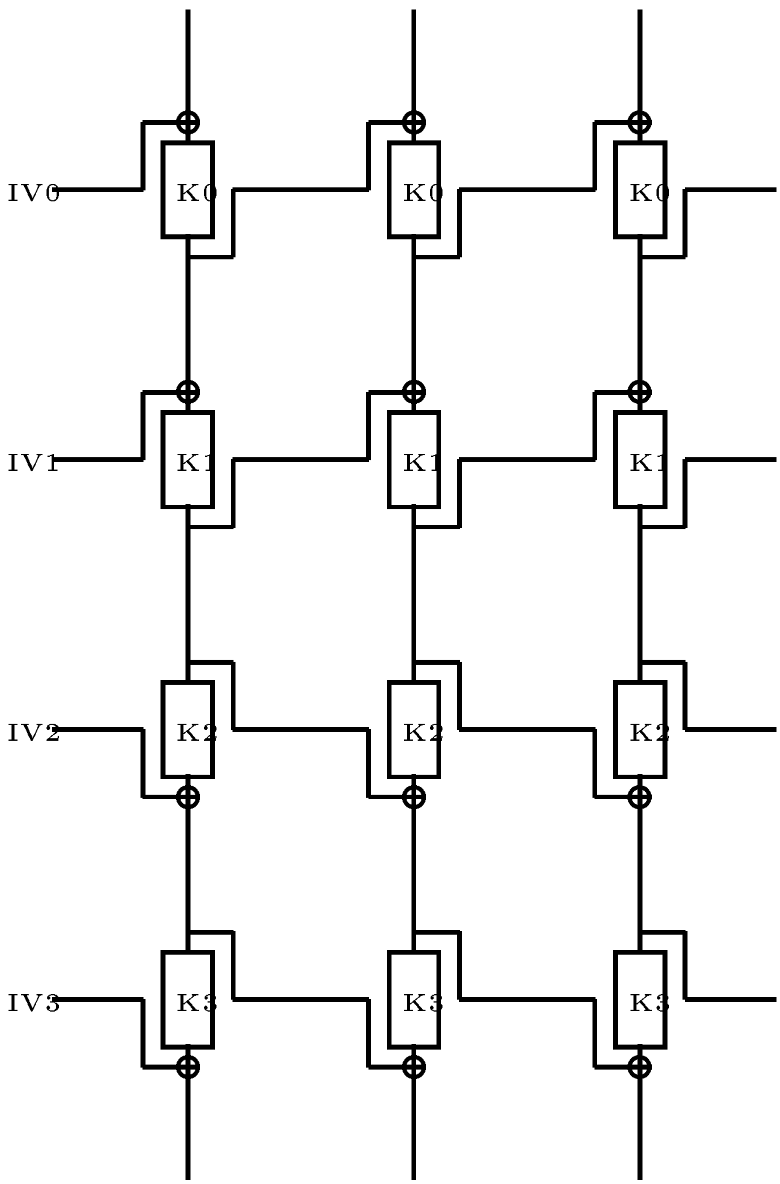


The CBC|CBC|CBC^{-1} |CBC^{-1} mode.

Narrow pipe attacks

Narrow pipe works: with 2^{32} chosen-ciphertexts, can find one collision, and learn $K3$.

P



C

The CBC|CBC|CBC^{-1} |CBC^{-1} mode.

Divide-and-conquer attacks

Divide-and-conquer attacks can break all modes of the form

1. OFB[M1,...,Mn] and M0| ... |Mn, where M$j \in$ {CFB,CFB^{-1}}.
   - Intuition: we have

     $$C_0 = P_0 \oplus E_{K0}(IV0) \oplus \ldots \oplus E_{Kn}(IVn).$$

2. OFB$\rightarrow$M1$\rightarrow$ ... $\rightarrow$Mn, where M$j \in$ {OFB,CBC,CBC^{-1},CFB,CFB^{-1}}.
   - Intuition: probe IVn to recover Kn, then recurse.

Complexity: $O(1)$ chosen-ciphertexts, $O(2^{56})$ work.

Narrow-pipe attacks

Can break

1. $\mathrm{CBC}|\mathrm{CBC}|\mathrm{CBC}^{-1}|\mathrm{CBC}^{-1}$
2. OFB[CBC,CBC]
3. OFB[CBC,CBC,CBC]
4. OFB[CBC, CBC,CBC^{-1}]

Complexity: 2^{32} chosen-ciphertexts, $O(2^{56})$ work (with one exception).

Summary of attacks

If multiple modes are micro-protocols, then chosen-IV attacks can be viewed as miniature protocol failures.

Can break all but two of Biham's nine proposed modes; need 1–2^{32} chosen-IV queries and $O(2^{56})$ work.
(Dented OFB[CBC,CBC,CBC^{-1}]. No results on OFB[CBC,CBC^{-1}].)

In short, adaptive chosen-IV chosen-ciphertext attacks seem very powerful.

But are they practical?

Countermeasures

Fix the multiple mode:

- Design principle: no IVs for internal chaining variables exposed.
  (Complicates the design.)

Fix the "protocol":

- Encrypt the IVs.
  (May still allow tampering.)
- MAC the IVs.
  (Won't stop known-IV attacks.)
- Maintain state across sessions; secret IVs.
  (Not always practical.)
- Something more sophisticated?
  (May add complexity...)

Different modes may require different fixes.

Conclusion: no silver bullet.

Contributions

- Chosen-IV attacks may allow one to probe inside the multiple mode.
- This shows another potential failure mode for these constructions.