

*Modes of Operation:
Where do we go from here?*

Bill Burr

william.burr@nist.gov

Aug 24, 2001



Overview

- Where are we now?
- What are the issues?
- What are the next steps in the process?

The Obvious Problem

- Five standardized DES Modes
 - ECB
 - CBC
 - CFB
 - OFB
 - *CBC MAC*
- Key and block size dependency problems for AES
- Only ECB is “fully parallelizable”
 - Gates are cheap and super scalar, super pipelined and vector processors are common

And there has been progress

- Precisely defined strict security properties
- Encrypting, authenticating modes
 - For about the cost of encryption alone
- Parallelizable modes
- Modes for particular applications

Obvious Answer

- Generalize existing modes for any block cipher
- Add counter mode
 - Facilitate pipelined or parallel implementations
- Hold a workshop on new modes
- We're doing most of the obvious things
 - “Basic” modes draft
 - Two workshops
 - 14 mode proposals plus AES hash

User Needs

- I claim that users want or need modes that are highly resistant to “practical” attacks.
 - Proofs of properties are one way to ensure this, but failure to meet particular properties may not lead to practical attacks
 - What’s impractical today might be practical in a decade
- Performance matters
- Interoperability matters
 - Lots of protocols and products out there
- Cost matters
 - Patent licenses

Issues for New Modes

- Basic Approach
 - Many or few modes?
 - Mandatory vs. recommended
 - Static or evolving?
 - Implementation Flexibility
- Implementation levels, modes vs protocols
 - Where is the divide?
- Mode Categories
 - What are we missing?
- Selection criteria and process

Issue: How Many New Modes?

- At least two alternative strategies:
 - Accept every arguably useful mode that seems sufficiently secure
 - fair - nobody with anything good gets excluded
 - Minimize the number of modes
 - promote interoperability
 - avoid insecure or dangerous alternatives
 - need to provide reasonable coverage of waterfront
- Surely we don't need 14 new modes
- Are there other modes we need?
 - Super-encryption
 - AES hash

Issue: Mandatory or Recommended

- Mandatory (FIPS)
 - Federal users who need other modes must waive FIPS
 - Inflexible, typically a 5 year change cycle
- Recommendation
 - More flexible, easier to accommodate evolution
 - Probably more risks
 - When do we move to more restrictive regime?

Issues: Implementation Flexibility

- Opposing comments
 - “too many options limits interoperability”
 - “too restrictive, limits utility”
- Minimize degrees of freedom to increase interoperability & reduce chance to go wrong, or
- Maximize freedom to allow more efficient, better tailored implementations
- More freedom => more chance to screw up
 - Testing is one answer, but
 - The more degrees of freedom the harder it is to test

Implementation Levels

- Algorithm
 - AES or any block cipher
- Mode
 - standardized ways to use the block cipher
- Protocol
 - A large number, many standards
- Application
 - This is what the user sees
 - The only level where the value or integrity requirements of data are known

Issues: Protocol Interactions

- Protocol designers often screw up security
 - Encryption and weak integrity checks invites attacks
 - Repeat cipher streams
- How much do we specify in modes, and how much do we leave to protocol designers?
- Can we fix this?
 - More comprehensive modes?
 - Lots of guidance?
 - More participation by crypto folks in protocol standards?

Mode Categories

- How many different mode categories do we need?
 - Authentication and encryption with one key
 - MAC
 - Hash
 - Super encryption

Mode Properties

- Performance
 - Number of block cipher operations
- Parallelizability
- Error expansion
- Crypto synchronization
- Stateful or stateless
- Formal security properties
 - How important, which ones?
- Other

Intellectual Property

- Patented modes are *very, very* unpopular
 - AES seems to be license free
 - Licensing crypto patents has been problematic
 - Patents may have little value if not in standards
 - Patents are always an issue in standards
 - IETF is very hostile to patented techniques
 - Higher costs for users
- Surely patents are a negative for any mode, but, if there is a huge advantage to a patented mode, and no god alternative, should we refuse to standardize it?

Observation

- FIPS 81, DES Modes of Operation, 1980
 - Didn't touch it for two decades
- Although modes do last a long time they are a rich, evolving subject
 - Lots of current development and progress
 - Can't expect to pick one or two new winners now and be done with it for another 20 years
- Analysis of modes is not simple
 - Complicated by assumptions about protocols
- We need an ongoing process or approach

Next Steps - Strawman

- Multipart Modes document
 - Don't try to do everything in one bundle
 - Add part 2, part 3, etc. as we go
 - Include new modes when they are “ripe”
 - Consider need for the mode and issues to be resolved
- Consider a separate guidance document on selecting and using modes.
- Continue to add modes as we resolve issues or get new proposals
- Regular workshops or meetings

Next Steps - Strawman

- Define major categories
 - One pass encrypt & authenticate
 - Improved MACs
 - Others (how many do we need?)
- Define Criteria
 - What are the essential properties for candidate modes?
 - By category

Discussion

