Truncated Differentials and Skipjack

Lars R. Knudsen
University of Bergen

M.J.B. Robshaw
RSA Laboratories

David Wagner
University of California, Berkeley

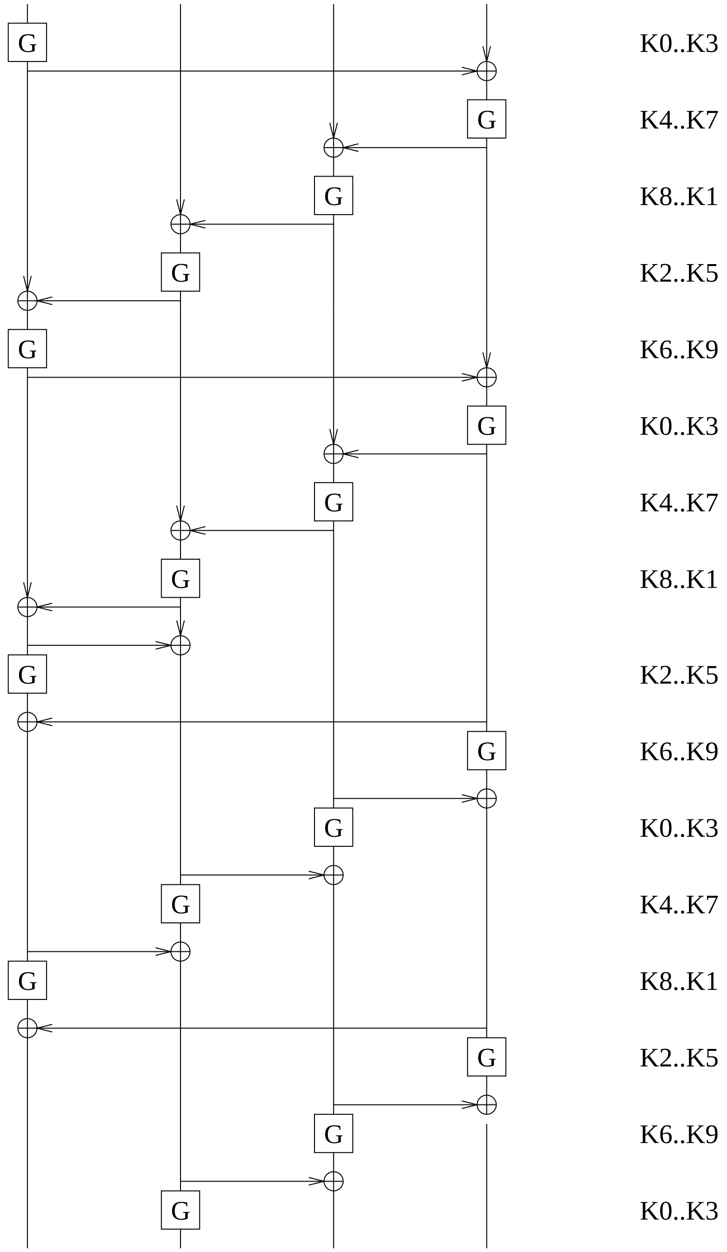
Organization

- Introduction to Skipjack
- Overview of approach and results
- Analysis: some truncated differentials, some attacks
- Related work, open problems, and conclusions

Skipjack

- Skipjack: yet another block cipher
  - 64-bit block
  - 80-bit key
  - 32 rounds
  - Two round-types, A-rounds and B-rounds; 8A 8B 8A 8B structure
- A fascinating object of study
  - Remarkably elegant design
  - Alien technology: NSA design, only recently declassified
  - Originally proposed for use in Clipper, at center of policy debate

The cipher (first 16 rounds)



Our approach

Central idea used in this work. *The high-level structure of Skipjack makes truncated differentials a powerful tool for the cryptanalyst.*

Ignore low-level details; attempt to validate the high-level structure of the cipher.

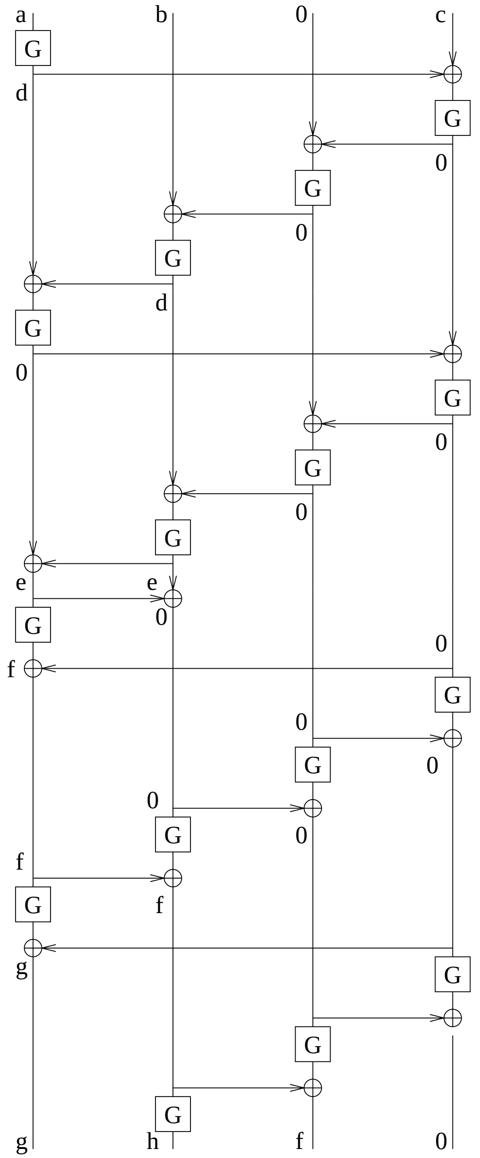
Overview of our results

Analysis of security and design of Skipjack:

- Long truncated differentials
  - Up to 24 rounds with probability 1!
- Truncated differential attacks
  - Attacks on up to 28 rounds
- Boomerang attacks
  - A new technique for attacking “from both ends at once”

$\Rightarrow$ structural properties of Skipjack that could be indicative of vulnerabilities

The first 16 rounds



$\Rightarrow$ A truncated differential of probability 2^{-32}.

Using the truncated differential

- The attack
  - **Encrypt:** encrypt 2^{17} texts with a fixed second word
  - **Filter:** look for pairs of ciphertexts with same fourth word
  - **Count:** look for first- and last-round subkey values suggested by at least two text-pairs

$\Rightarrow$ breaks first 16 rounds with 2^{17} texts, 2^{34}–2^{49} time

Observations

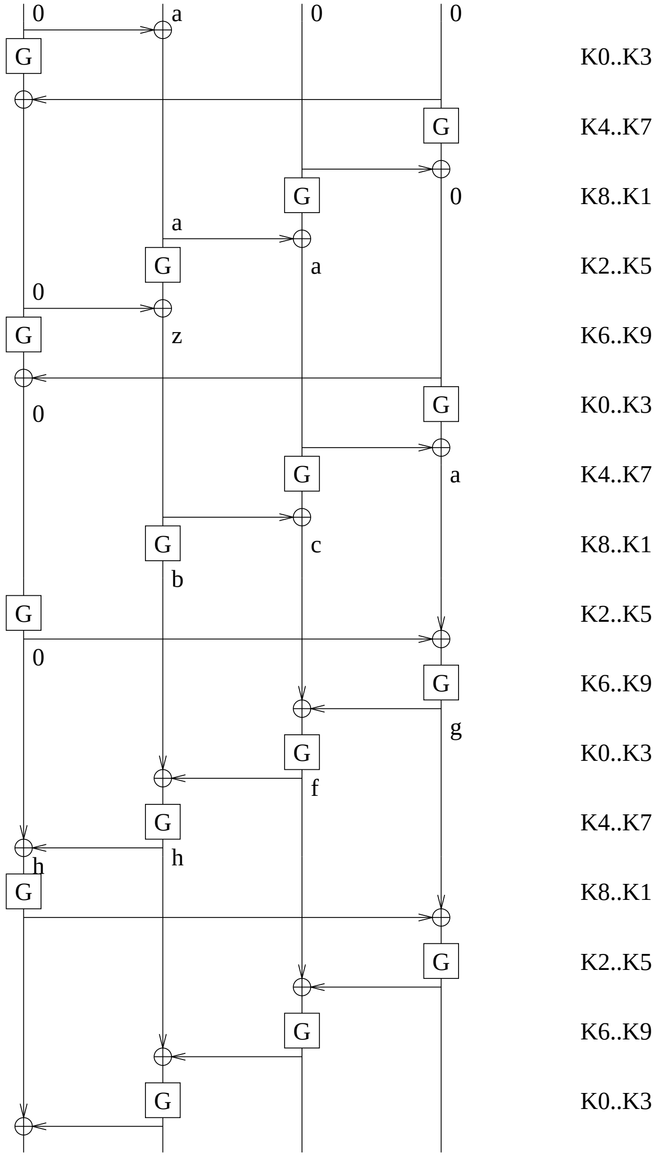
What happened?

- B-rounds have bad diffusion in the forward direction
- Bad interaction at boundary between A- and B-rounds

Truncated differentials beat conventional differential cryptanalysis:

- Truncated differentials model the high-level structure of the cipher
  $\Rightarrow$ higher probability differentials (up from $2^{-52.1}$ to 2^{-32})
- Structures allow a more efficient use of chosen texts
  $\Rightarrow$ $2^{16}\times$ fewer chosen plaintexts needed

The middle 16 rounds



⇒ A 12-round truncated differential of probability 1.

The attack

- **Encrypt:** encrypt 2 texts differing only in their second word
- **Count:** do a 7-R (!) analysis

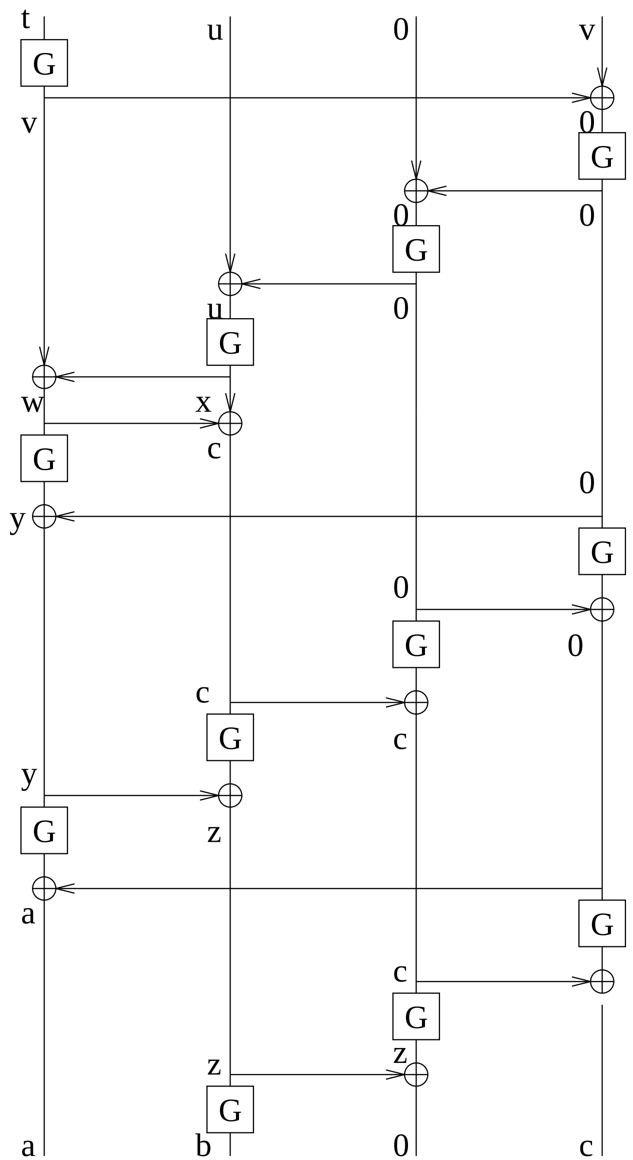
$\Rightarrow$ breaks middle 16 rounds with *two* texts and 2^{47} time

Observations

- The round ordering matters
  - Start with B-rounds yields longer differentials
  - Ending with A-rounds lets you look deeper into cipher (7 rounds!)

- The middle 16 rounds are *very* weak
  - Breakable with *two* texts: close to the Shannon bound!
  - Compare: best known attack on half of DES takes 2^8 texts

28 rounds



Concatenate with 16-round truncated diff. to get 28 rounds with prob. 2^{-64}.

Attack

- Can break 28 rounds with 2^{41} chosen texts
  - Use the 28-round truncated differential with probability 2^{-64}
  - Count on first- and last-round subkeys

- Extensions to full 32 rounds?
  - There are 32-round truncated differentials with same probability
  - But filtering is worse and counting requires guessing more key bits
    $\Rightarrow$ Keeping time complexity under 2^{80} is a real challenge

  $\Rightarrow$ Extending the attack looks difficult but not a priori impossible

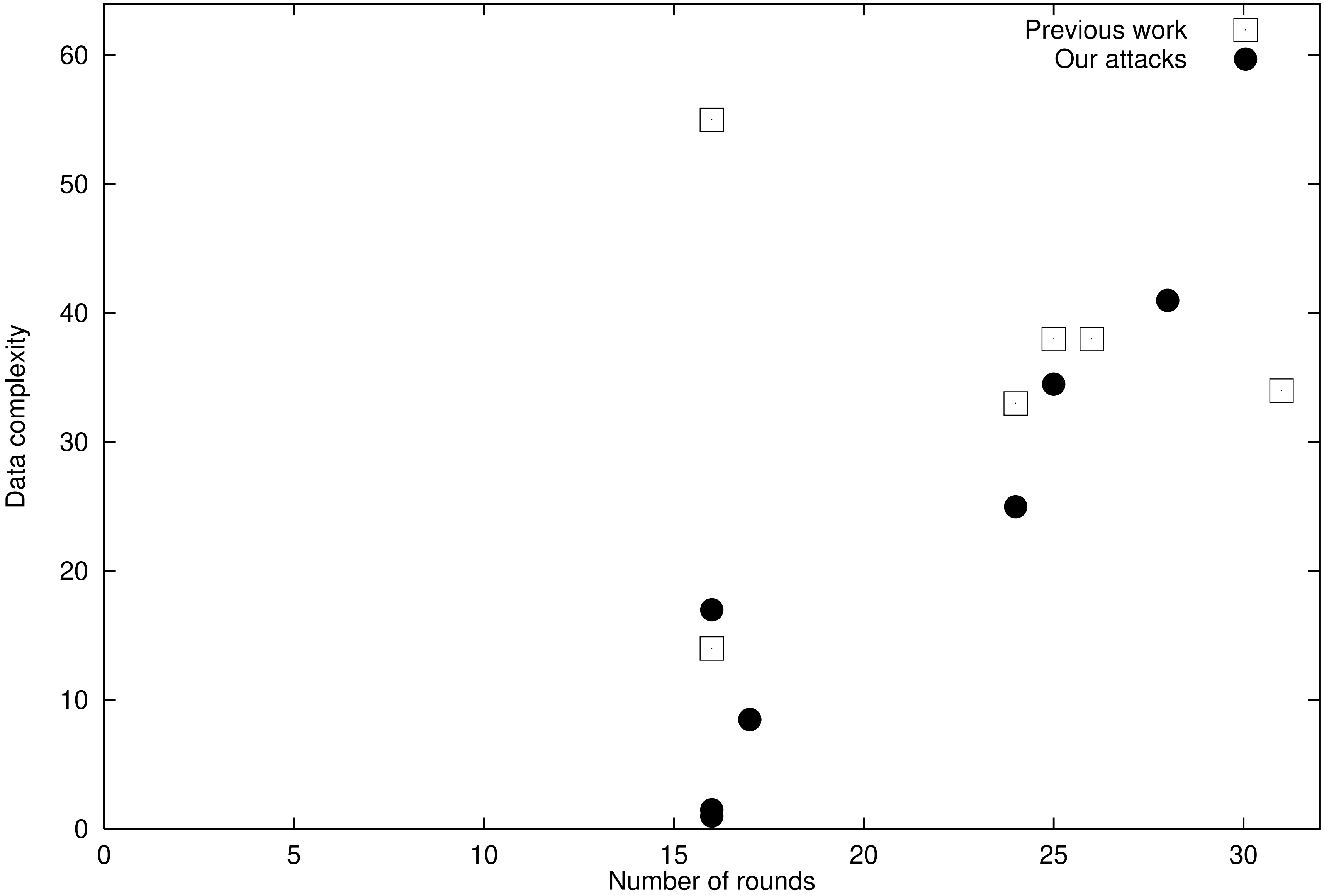
Open problems

- Extensions to attacks on the full cipher?
- Validation of the design?
- Proofs of security?
- Connections with stream ciphers?

Summary of attacks

Variant	Complexity	Authors	Attack technique
First 16 rounds	2^{55} texts	[BBDRS]	Conventional differential attacks
First 16 rounds	2^{14} texts	[BBDRS]	Yo-yo game
Middle 24 rounds	2^{33} texts	[BBS]	Impossible truncated differentials
Middle 25 rounds	2^{38} texts	[BBS]	Impossible truncated differentials
31 rounds	2^{34} texts	[BBS]	Impossible truncated differentials
32 rounds -3XOR	2^{9} texts	[BBDRS]	Truncated differentials
First 16 rounds	2^{17} texts	us	Truncated differentials
Middle 16 rounds	2 texts	us	Truncated differentials
Middle 24 rounds	2^{25} texts	us	Boomerang attack
Middle 25 rounds	$2^{34.5}$ texts	us	Boomerang attack
Last 28 rounds	2^{41} texts	us	Truncated differentials

Graphing the best attacks



Conclusions

- High-level structure of cipher has some surprising properties
- Truncated differentials are a powerful tool for analysis of Skipjack
  - Can break 28 rounds with 2^{41} texts...
  - ...and can break 16 rounds with only *two* texts
- But an attack on the full cipher remains elusive