# *LOKI97 - AES1*

Dr Lawrie Brown
Australian Defence Force Academy

Drs Josef Pieprzyk, Jennifer Seberry
CCSR, University of Wollongong

# *Introduction*

- LOKI97
  - new 128-bit private key block cipher
  - based on earlier LOKI89 and LOKI91
  - traditional Feistel S-P design
  - AES candidate

# *Previous Work - LOKI89*

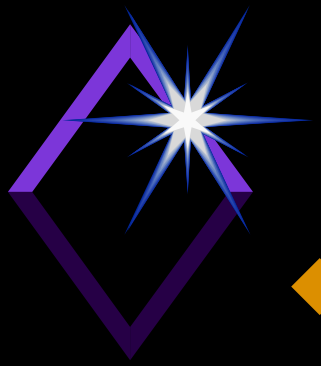
- 64-bit private key block cipher
- Brown, Pieprzyk, Seberry 1989/90
  - see Brown PhD thesis
- Biham and Shamir, Knudsen
  - differential cryptanalysis of reduced rounds
  - full version secure

# *Previous Work - LOKI91*

- Redesigned in 1991
  - by Brown, Kwan, Pieprzyk, Seberry
  - better round function and key schedule

# *Previous Work - LOKI91*

- Knudsen, Biham, Tokita et al
  - differential cryptanalysis of reduced rounds
  - linear cryptanalysis of reduced rounds
  - full version secure from DC *and* LC
  - some key schedule weaknesses
    - effective key size approx 60 bits



# *Design Considerations*

- Motivated by Knudsen 93
  - no simple relations (vis data and key)
  - all keys are equally good
  - resistant to differential attacks
  - resistant to linear attacks

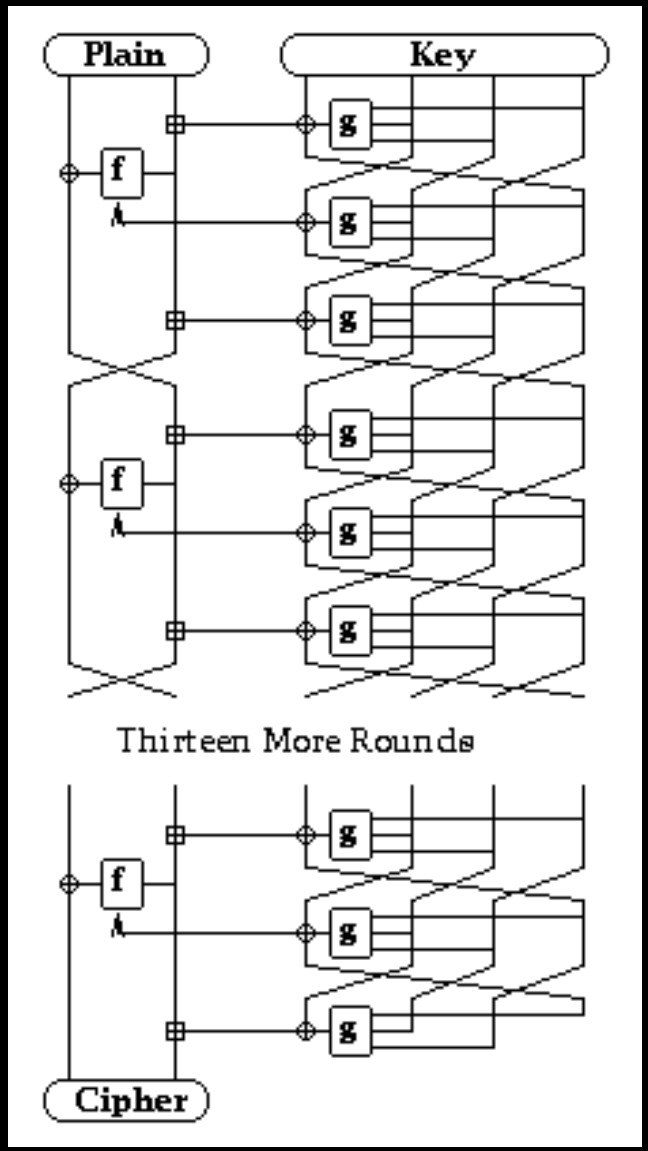
# *(Further) Design Considerations*

- non-linear key schedule
- highly non-linear round function
- efficient implementation with tables

# *LOKI97 Overview*

- LOKI97 is
  - private key Feistel S-P block cipher
  - 128-bit data
  - 256-bit key schedule initialised from 128, 192, 256-bit keys
  - 16 round data computation using a complex highly non-linear function
    - two layers of designed S-P per round
  - same function also used in key schedule

# *LOKI97 Overview*



# *LOKI97 Main Details*

- data computation

  $R_i = L_{i-1} \text{ xor } f(R_{i-1} + SK_{3i-2}, SK_{3i-1})$

  $L_i = R_{i-1} + SK_{3i-2} + SK_{3i}$

- key schedule

  $SK_i = K4_{i-1} \text{ xor}$

  $f(K1_{i-1}+K3_{i-1}+nD, K2_{i-1})$

  $K4_i=K3_{i-1}, K3_i=K2_{i-1}, K2_i=K1_{i-1}, K1_i=SK_i$

  $D = \text{floor}( (\text{sqrt}(5)-1).2^{63} )$

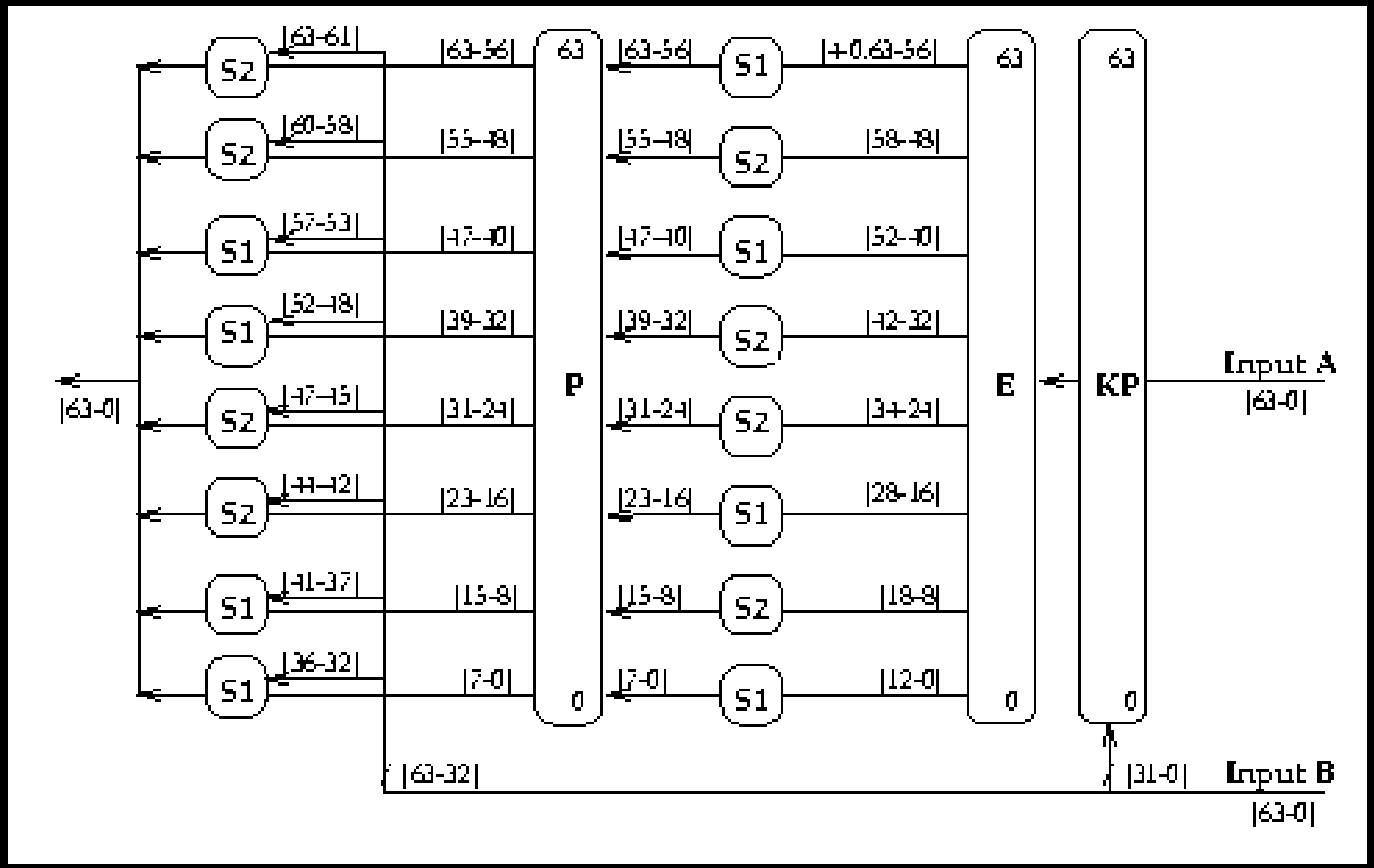
# *LOKI97 Round Function*

- highly non-linear 64-bit function

  *f*(A,B) = Sb(P(Sa(E(KP(A,B)))),B)

- 2 columns each of 2 S-boxes
  - Sa = [S1,S2,S1,S2,S2,S1,S2,S1]
  - Sb = [S2,S2,S1,S1,S2,S2,S1,S1]
- regular perm P diffuses Sa outputs
  - fans S-box out to cover all Sb inputs
- keyed permutation KP to exchange selected pairs of bits set by input B

# LOKI97 Function f(A,B)

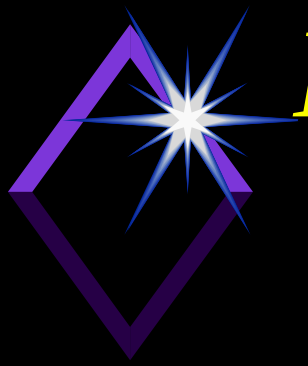


# *Rationale for S-boxes*

- Want S-boxes which must
  - be balanced
  - be highly non-linear
  - satisfy strict avalanche criteria (SAC)
  - have good XOR profile

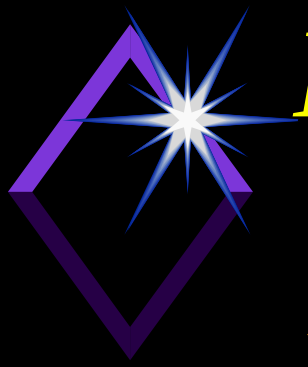
# *Rationale for S-boxes*

- Cubing in odd Galois fields is proven to be good
  - $S(x) = x^3 \bmod p$, $p$ irreducible polynomial in $GF2^n$
  - used n = 11 and 13
  - inverted input, truncated result to 8



# *Preliminary Analysis: Key Schedule*

- no general linear relations for keys
  - no keys with repeated subkeys, eg 0
  - the first 4 subkeys can be coerced to 0 by solving suitable key schedule equations



# *Preliminary Analysis: Key Schedule*

- the first 4 subkeys can be coerced to 0 by solving the key schedule equations
  - SK1,2,3=0,
    K=[*f*(*f*(*f*(3D,0)+2D,0)+D,*f*(3D,0)) | *f*(*f*(3D,0)+2D,0) | *f*(3D,0) | 0]
  - SK1=0, K=[*f*(D,0) | 0 | 0 | 0]
  - SK1,2=0,
    K= *f*(*f*(2D,0)+D,0) | *f*(2D,0) | 0 | 0]

# *Preliminary Analysis: S-Boxes*

- XOR profiles very flat
  - S1 peak 64 (of 8192), zero peak 32
  - S2 peak Avalanche
  - 32 (of 2048), zero peak 16
  - ie standard 2 round characteristic has maximum Pr(1/256)
  - exhaustively tested all 1 bits changes
  - small number of 0 or 1 bit changes
    - similar to LOKI91

# *Preliminary Analysis: DC and LC*

- Rijmen / Knudsen have suggested
  - DC attack using 2R characteristic via MSB
    - since XOR unchanged under addition
  - LC attack using a bias in *f* in directly keyed Sb layer

# *Possible Changes*

- shift E down 2 bits, so MSB (63) is duplicated
  - should thwart DC attack
- consider alternatives for keying Sb to remove bias

# *Conclusions*

- overview of LOKI97 design
  - previous work
  - rationale
  - goals
  - initial analysis
  - description
  - suggested alterations

# *Further Information*

- on AES

  http://www.nist.gov/aes/

- on LOKI97

  http://www.adfa.edu.au/~lpb/research/loki97/