Rotational cryptanalysis of ARX

Dmitry Khovratovich, Ivica Nikolić

University of Luxembourg

Seoul, FSE'10
10 February 2010

ARX

Addition-Rotation-XOR (and constants)

- Addition for nonlinearity;
- Rotation for intra-word diffusion;
- XOR for inter-word diffusion and linearity (!).

Using ARX:

- MD4-family (1990-92);
- SHA-0/1/2 (1994-2001).

SHA-3 ARX candidates:

- BLAKE;
- Cubehash;
- Skein.

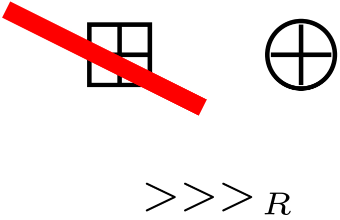
$$\boxplus \qquad \oplus$$

$$>>>_R$$

RX

What if we remove the addition?

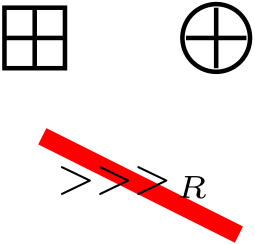
- The system is linear;
- Easy to solve.



AX

What if we remove rotation?

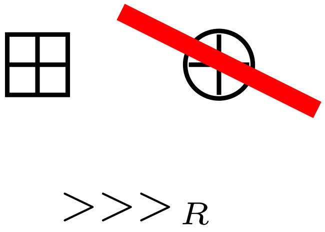
- MSB do not influence LSB;
- One-direction diffusion;
- Easy to break gradually (see also preimage attack on SHA-1 by De Cannière and Rechberger).



AR

What if we remove XOR?

- Formally XOR can be realized by $\{+, \ggg\}$ and constants.
- Though it is costly;
- Small systems are vulnerable.



Cryptanalysis of AR

Idea:

- Approximate $\boxplus \pmod{2^n}$ with $+$;
- Approximate $\lll_r$ with $2^r \odot \pmod{2^n - 1}$ (see also mod n cryptanalysis by Kelsey-Schneier-Wagner);

Cryptanalysis of AR

Idea:

- Approximate $\boxplus$ (mod 2^n) with $+$;
- Approximate $\lll_r$ with $2^r \odot$ (mod $2^n - 1$) (see also mod n cryptanalysis by Kelsey-Schneier-Wagner);
- All the computations are now modulo $2^n - 1$;
- This a linear approximation.

An AR-system with Q additions can be approximated with linear function with probability 2^{-Q}.

ARX without constants

ARX without constants?

- $F(0) = 0$;
- Symmetry patterns in symmetrical designs;
- What else?

Cryptanalysis of ARX and related systems

Collisions:

- Additive differentials (Dobbertin, Wang);
- Solving systems of equations (Dobbertin for MD5, van Rompay et al. for HAVAL, Mendel et al. for Tiger, Nikolić-Biryukov for SHA-2);
- Linearization (Chabaud-Joux, Biham et al., Brier et al.);
- Auxiliary differential paths (tunnels, submarines, boomerangs, and many others).

Cryptanalysis of ARX and related systems

Preimages:

- Local collision techniques (Leurent, Sasaki-Aoki);
- Splice-and-cut for the meet-in-the-middle (Aumasson-Mendel-Meier, Sasaki-Aoki);
- Gradual state recovery (De Cannière-Rechberger for SHA-0/1, Aumasson et al. for DynamicSHA).

Rotational cryptanalysis

Steps towards

- Biham used rotated related keys in the attack on LOKI (1993).
- Dobbertin and Wang used additive differentials, which go through XORs and rotations.
- Kelsey, Schneier, and Wagner attacked rotation-addition (AR) systems with mod n cryptanalysis (1999).
- Daum studied the carry behaviour and probabilities of the rotation w.r.t. addition in the thesis (2005).
- Rotational cryptanalysis of SEA was considered by the designers (2006).
- Modified Serpent was attacked with rotational cryptanalysis (Dunkelman-Indesteege-Keller, 2008).

Rotational pairs

Definition

Consider a *rotational pair* of inputs $(X, \overrightarrow{X})$:

$$\overrightarrow{X} = X \ggg_r .$$

ARX:

- **[X]**: $\overrightarrow{X \oplus Y} = \overrightarrow{X} \oplus \overrightarrow{Y}$;
- **[R]**: $\overrightarrow{X} \ggg_{r'} = \overrightarrow{X \ggg_{r'}}$.

Preserved by XOR and rotation, and independent of rotation distance.

Properties

- **[A]**: Preserved by $\boxplus$ with high probability:

$$\mathbb{P}_r\left[\overrightarrow{X \boxplus Y} = \overrightarrow{X} \boxplus \overrightarrow{Y}\right] = \frac{1}{4}(1 + 2^{r-n} + 2^{-r} + 2^{-n}).$$

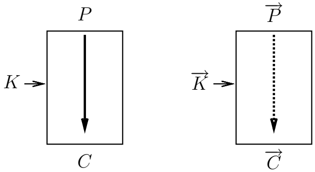
For small r and large n:

r	$\mathbb{P}_r$	$\log_2(\mathbb{P}_r)$
1	0.375	−1.415
2	0.313	−1.676
3	0.281	−1.831
	...	
$n/2$	0.25	−2

- **[C]**: Changed by a constant addition:

$$\overrightarrow{X \oplus C} = \overrightarrow{X} \oplus C \oplus (C \oplus \overrightarrow{C})$$

Attack



- Rotate all inputs;
- Check whether the outputs are rotated.
- If there is no constants

$$\mathbb{P} \approx (p_r)^Q,$$

Q is the number of additions.

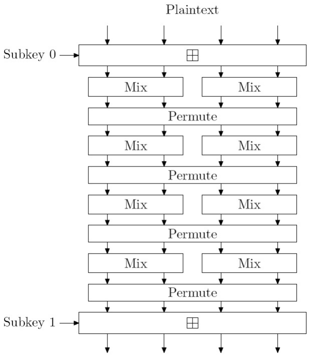
Advantages

Advantages:

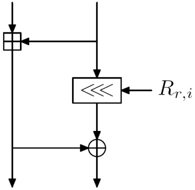
- The structure is not important;
- Any set of rotation constants in the primitive is admissible (e.g. the recent Skein tweak does not help).
- Round probability does not grow.

Cryptanalysis: Threefish/Skein

Threefish/Skein

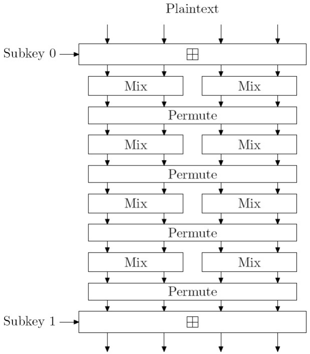


MIX:

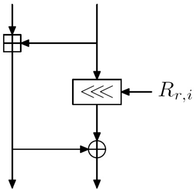


- State and key of N 64-bit words;
- $N/2$ additions per round;
- Key addition every 4 rounds;

Threefish/Skein



MIX:



- 72–80 rounds in total;
- Symmetry and slide countermeasures:
  - Key addition constants (1–18);
  - One subkey is xored with $\lfloor 2^{64}/3 \rfloor$.

Attack model

We choose the strongest model:

- Attack the underlying block cipher (Threefish) for simplicity;
- The secret-key setting;
- $0R$-attack.

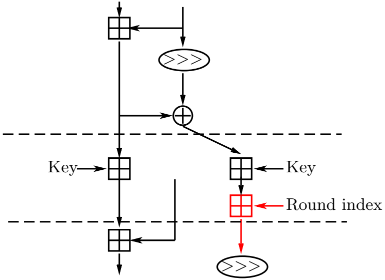
In other models more rounds can be broken.

Simple attack

Simple attack

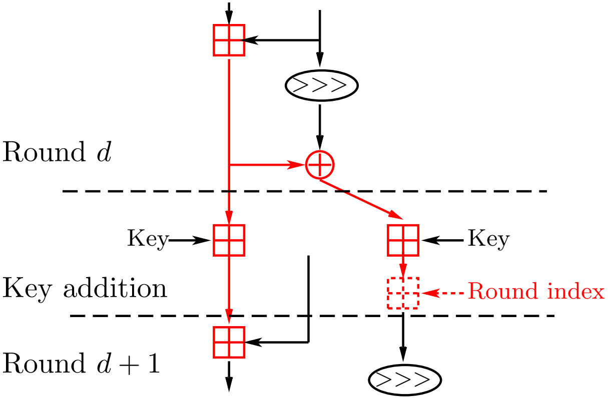
- Require all the variables to be rotated;
- Round constants introduce an error;
- Error is rotated immediately.

Does not work.



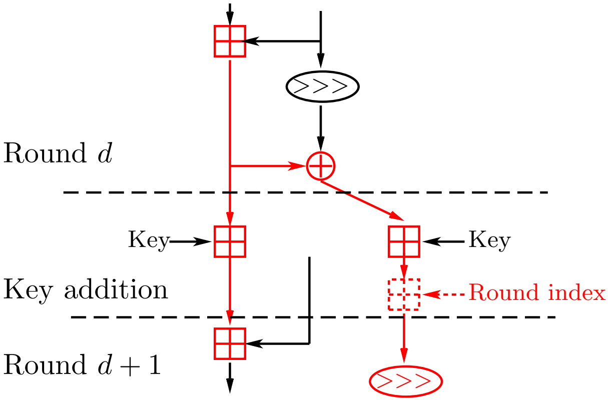
Attack

- Rotate by 2 bit to cancel $\lfloor 2^{64}/3 \rfloor$ (invariant);
- Small constants can be corrected:



Attack

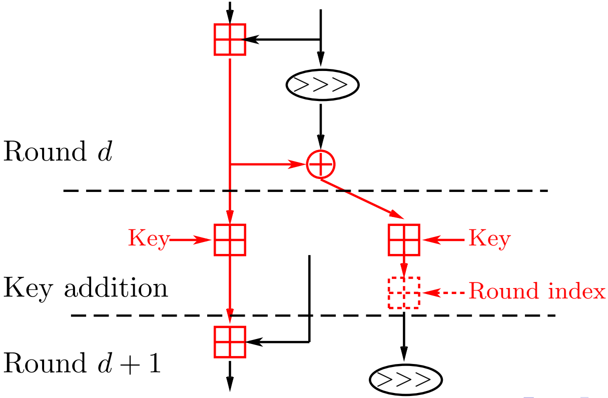
For large round indices it is impossible:



Rotational errors

Idea: introduce rotational errors in the key words:

$$K_i' = \overrightarrow{K_i} \oplus e_i$$



Summary

Threefish-256 (72 rounds)		
24	Related-key differential	[Submission]
39	**Related-key rotational**	-
Threefish-512 (72 rounds)		
25	Related-key differential	[Submission]
32	Related-key boomerang	[Aumasson et al.]
33	Related-key boomerang	[Chen-Jia]
42	**Related-key rotational**	-
35	Known-related-key distinguisher	[Aumasson et al.]
Threefish-1024 (80 rounds)		
26	Related-key differential	[Submission]
43.5	**Related-key rotational**	-

Other applications

Other applications

- All the bitwise functions preserve the rotational pair (those MD5 and SHA-0/1);

Other applications

- All the bitwise functions preserve the rotational pair (those MD5 and SHA-0/1);
- Rotation-invariant transformations (Keccak, RadioGatun) — with probability 1, so no way to cancel a constant;

Other applications

- All the bitwise functions preserve the rotational pair (those MD5 and SHA-0/1);
- Rotation-invariant transformations (Keccak, RadioGatun) — with probability 1, so no way to cancel a constant;
- Rotational pair can form a boomerang quartet in the middle;

Other applications

- All the bitwise functions preserve the rotational pair (those MD5 and SHA-0/1);
- Rotation-invariant transformations (Keccak, RadioGatun) — with probability 1, so no way to cancel a constant;
- Rotational pair can form a boomerang quartet in the middle;
- S-boxes?