Different attacks on Salsa and ChaCha Cipher with attack complexity

- Aumasson et al. (FSE 2008)

  - 2^{251} on Salsa20/8,
  - 2^{248} on ChaCha7,
  - 2^{151} on Salsa20/7,
  - 2^{139} on ChaCha6.

  Idea: In this the authors introduced the concept of Probabilistic Neutral Bits (PNBs). Using this idea authors divided the key bits into two types *significant key bits* and *non-significant key bits* based on the amount of influence which each bit of the key has on the output function. Using this they proposed a meet-in-the-middle attack.

- Shi et al. (ICISC 2012)

  Margin of improvement:

  - 2^{1} on Salsa20/8 (2^{251} to 2^{250}),
  - $2^{1.5}$ on ChaCha7 (2^{248} to $2^{246.5}$),
  - 2^{3} on Salsa20/7 (2^{151} to 2^{148}),
  - 2^{3} on ChaCha6 (2^{139} to 2^{136}).

  Idea: The authors modified the PNB-based attack slightly by introducing the concept of Column Chaining Distinguisher.

- Maitra et al. (WCC 2015)

  Margin of improvement:

  - $2^{2.8}$ on Salsa20/8 (2^{250} to $2^{247.2}$).

  Idea: The authors use the similar attack idea as above, but provide some better result by using better set of PNBs and better distinguishers.

- Maitra (DAM 2015)

  Margin of improvement:

  - $2^{1.7}$ on Salsa20/8 ($2^{247.2}$ to $2^{245.5}$),
  - $2^{7.5}$ on ChaCha7 ($2^{246.5}$ to 2^{239}).

Idea: The author introduced the idea of Right-pair (chosen-IV attack). Author showed that if the IV can be chosen in such a way that the difference propagation in the first round is minimum, we can observe improvement in the bias of the distinguisher. Thus, attack complexity decreases.

- Choudhuri et al. (FSE 2017)

  Margin of improvement:

  - to $2^{0.6}$ on Salsa20/8 ($2^{245.5}$ to $2^{244.9}$),
  - to $2^{1.3}$ on ChaCha7 (2^{239} to $2^{237.7}$),
  - to 2^{11} on Salsa20/7 (2^{148} to 2^{137}),
  - to 2^{20} on ChaCha6 (2^{136} to 2^{116}).

  Idea: The authors found correlation between a single bit of lower round with a linear combination of bits of the higher round. Thus, from the existing differential attack they generated a linear extension, which is essentially a differential-linear attack. The key recovery attack process remains same as before.

- Dey et al. (DAM 2017)

  Margin of improvement:

  - $2^{1.2}$ on Salsa20/8 ($2^{244.9}$ to $2^{243.67}$),
  - $2^{2.5}$ on ChaCha7 ($2^{237.7}$ to $2^{235.2}$).

  Idea: In this author provided a improved algorithm by Greedy approach to find probabilistic neutral bits, thus achieved a better set of PNBs. The online attack procedure remains same.

- Dey et al. (AMC 2019)

  Margin of improvement:

  - $2^{0.46}$ on Salsa20/8 ($2^{243.67}$ to $2^{243.23}$),
  - $2^{0.42}$ on ChaCha7 ($2^{235.2}$ to $2^{234.78}$).

  Idea: Analyzing how to assign values to the PNBs in order to improve the backward bias. No change in the remaining attack technique.

- Beierle et al. (CRYPTO 2020)

  Margin of improvement:

  - $2^{38.6}$ on ChaCha6 (2^{116} to $2^{77.4}$),
  - $2^{3.92}$ on ChaCha7 ($2^{234.78}$ to $2^{230.86}$).

  Idea: In this they discovered a single bit distinguisher in the 3.5 round of ChaCha. Also produced a differential linear partial key recovery attack on 6-round ChaCha. For 7-round ChaCha, they used the existing attack technique.

- Coutinho et al (EUROCRYPT 2021)

  Margin of improvement:

  - $2^{26.4}$ on ChaCha6 ($2^{77.4}$ to 2^{51}),
  - $2^{6.86}$ on ChaCha7 ($2^{230.86}$ to 2^{224}).

  Idea: In this they discovered few more single bit distinguisher in the 3.5 round of ChaCha. Using linear approximation techniques similar to the Choudhuri et al., they produced distinguishers for 7-round ChaCha. They key recovery attack technique remains same, except that they used a better distinguisher.

- Dey et al. (EUROCRYPT 2022)

  Margin of improvement:

  - $2^{2.05}$ on ChaCha7 (2^{224} to $2^{221.95}$).

  Idea: In this author portioned the key bits into memory and non-memory key bits. Thus, they use a time-memory tradeoff technique. Also, provide some modification in the PNB finding algorithm.

- Coutinho et al. (JOC 2023)

  Margin of improvement:

  - 2^{10} distinguishing attack on ChaCha7 (2^{224} to 2^{214}),
  - $2^{27.61}$ key recovery attack on Salsa20/8 ($2^{243.23}$ to $2^{215.62}$),
  - $2^{27.76}$ distinguishing attack on Salsa20/8 ($2^{244.9}$to $2^{217.14}$).

Idea: Used an idea called Bidirectional Linear Expansions (BLE) where with the help of piling up lemma, they theoretically estimate a single bit distinguisher bias in a higher round from the biases of a few bits in a smaller round. Then, they linearly extend that distinguisher to higher rounds by some modifications of the previously existing extension techniques.

- Dey et al. (FSE2023)

  Margin of improvement:

  - $2^{5.2}$ on ChaCha6 ($2^{104.68}$ to $2^{99.48}$).

  Idea: The authors provided a multi-step key recovery attack, using multiple distinguishers, and thus multiple set of PNBs.

- Our Work

  Margin of improvement:

  - $2^{21.19}$ on Salsa20/8 ($2^{217.14}$ to $2^{195.95}$) and $2^{40.23}$ on Salsa20/8 ($2^{236.15}$ to $2^{195.95}$).

    (Note that as we have mentioned in our work that the corrected complexity of JOC 2023(by Coutinho et al.) is $2^{236.15}$ instead of $2^{217.14}$.)

  - $2^{6.32}$ on Salsa20/7 (2^{107} to $2^{100.68}$). (128-bit key version)

  First-ever Attack:

  - $2^{253.80}$ on Salsa20/8.5, (256-bit key version)
  - $2^{116.62}$ on Salsa20/7.5. (128-bit key version)