A Study of Practical-time Distinguishing Attacks Against Round-reduced Threefish-256

Aron Gohr
Bundesamt für Sicherheit in der Informationstechnik (BSI)

March 22, 2012

Short summary I: Threefish

Basic data on Threefish:

- Threefish is a tweakable block cipher and the cryptographic core primitive of the Skein hash function.
- Key and block sizes of 256, 512 or 1024 bits, 128-bit tweak.
- Best attacks on Threefish: related-key boomerang attacks. Introduced by Aumasson, Calik, Meyer, Özen, Phan, Varici [1], further studied by others [2, 5].
- Complexity: 2^{474} (34 rounds of Threefish-512, key recovery, [2]), 2^{398} (34 rounds of Threefish-512 with old rotation constants, distinguisher, [1]), 2^{234} (31 rounds of Threefish-256, distinguisher, [5]).

Short summary II: Motivating questions, setting

Motivating questions of this paper:

- What can we still do if we require practical time and memory complexity?
- How do predictions of attack complexity relate to measured attack complexity in this case?

Setting:

- Secret-key distinguishing attacks.
- Chosen upper limit of practicality: 2^{45} oracle query complexity.

Short summary III: Attacks

- Focus on reduced-round, practical time variants of the best known theoretical attacks (related-key boomerang attacks).
- Use multiple differential paths in the middle of the cipher (as in [2]), detect truncated state instead of full differential after decryption step to bring down attack complexity. Estimate rectangle attack complexity by empirical evaluation of a sub-boomerang in the middle.
- Use $\boxplus$-differentials (as in [2]) to pass subkey additions at no cost. Use exact computations of differential transition probabilities for bitwise additions, rotations.

Short summary IV: Results

- Attack cost estimates quite good on a round-by-round basis. Cost estimates for the full trail noticeably worse but still useful.
- Main attack covers 27 rounds of Threefish-256 at estimated cost of $2^{40.2}$ boomerang evaluations.
- First 26 and last 23 rounds of main attack empirically verified.

Structure of Threefish

The n-th round R_n of Threefish has the following structure:

$$R_n = \begin{cases} \mathrm{Permute} \circ \mathrm{Mix}, & n \not\equiv 0 \bmod 4 \\ \mathrm{Permute} \circ \mathrm{Mix} \circ \mathrm{AddSubKey}, & n \equiv 0 \bmod 4, \\ \mathrm{AddSubKey} \circ \mathrm{Permute} \circ \mathrm{Mix}, & \text{final round.} \end{cases}$$

where $\mathrm{Permute}$ is a reordering of the 64-bit words of the state and Mix is the parallel application of several (almost) copies of a simple nonlinear transform $\{0,1\}^{128} \to \{0,1\}^{128}$ built from one addition, one rotation and one XOR (ARX).
Current paper only looks at Threefish-256: state consists of four 64-bit words, 2 Mix transforms per round.

Differential paths through Threefish

Which kind of differentials should one use for Threefish?

- $\oplus$-paths: only one nonlinear operation per Mix transform. But: modular additions with secret subkeys may incur significant costs at the beginning and the end of the cipher.
- $\boxplus$-paths: subkey additions are completely linear, rotations in Mix transforms have still very good differential behaviour.

Present work uses $\boxplus$-differentials.

Calculating differential path probabilities

Given a differential path, do the following:

- Calculate input and output differences to bitwise additions and rotations in the Mix transforms.
- Calculate exact probabilities for these differential transitions.
- Assume independence of these events and multiply.

To execute the second step, closed formulas from the thesis of Daum [3] were used for rotations and a method due to Lipmaa, Wallén, Dumas [4] (esssentially counting the paths to the accepting state in the state transition graph of a suitable finite state machine) for the additions.

Round-by-round probabilities in an example path I

Compare round-by-round predictions and measurements in an actual four-round path from one of the attacks:

Round r	$log_2(\mathbb{P}_r)$ empirically	$log_2(\mathbb{P}_r)$ predicted
Rotations	-1.098	-1.098
0	-20.65	-20.63
1	-7.97	-7.95
2	-3.17	-3,21
3	-1.00	-1

Round-by-round probabilities in an example path II

Key points to remember:

- Agreement even on round-by-round-basis is not always *that* good.
- The resulting prediction for the four-round path in question is noticeably worse: prediction is $\approx 2^{-33}$, measurement gives $\approx 2^{-29}$.
- Still overall this very simple model performs well.

Attack setting

- Attacks considered are *secret-key distinguishing attacks* using related-keys or related-tweaks.
- Use bitwise differences for related-keys, related-tweaks and modular differences for the message.
- Pass the last few rounds of the backwards direction of the boomerang by using a truncated differential.

Short introduction to boomerang attacks

- First basic idea: suppose you have a right input pair $M, M + \alpha$ for a differential transition $E : \alpha \to \delta$. Maybe if we change M a little bit, we can find another satisfying input pair $M', M' + \alpha$?
- Second basic idea: of course we may also manipulate $E(M), E(M) + \delta$ instead of $M, M + \alpha$ and hope that upon decryption of this we get with high probability another pair with difference α.
- Boomerang attack provides a framework where exactly this happens. Conditions: $E = E_1 \circ E_0$, high probability paths $E_0 : \alpha \to \beta$, $E_1^{-1} : \delta \to \gamma$, encryption and decryption access to E.

Best known attacks on Threefish

- The best attacks known are related-key, related-tweak boomerang/rectangle attacks.
- Basic structure of the forward differential in these attacks:
  - Use short initial differential to obtain with high likelihood a state collision after round four.
  - Use key schedule to obtain a subkey collision in round eight.
  - Extend the differential by some further rounds until the meet-in-the-middle-point of the boomerang.
- Backwards differential: same structure.

Main attack of the present paper

- Related-key rectangle attack: we do not care about what happens around the meet-in-the-middle point of the boomerang.
- In the decryption direction, detect a truncated difference with 25 bits defined.
- Truncated state very likely ($\mathbb{P} \approx 0.98$) if in the decryption direction things went well up to round 12.
- This happens with likelihood $\approx 2^{-40}$ for the 27-round attack.
- Therefore, a retesting method is needed.

Retesting

If the desired truncated difference is found after executing the boomerang test, do:

- Generate a new boomerang input pair from the candidate.
- Test that one.
- Repeat this a few thousand times until you either confirm or abandon the candidate pair.

New input pairs can e.g. be generated using neutral bits. In general, many strategies for producing such pairs are possible.

Related-tweak attack

- If we are not allowed to use related-keys but only related-tweaks, we can no longer sustain state collisions for eight rounds but can choose better initial and final differentials.
- Result: fixed-key, related-tweak attack of the same structure on 19 rounds at cost of $\approx 2^{26.3}$ rectangle test evaluations without a retesting procedure.
- Complexity predictions work reasonably but not exceedingly well in this example too.

Conclusions

- Practical-time distinguishing attacks possible against at least 27 rounds of Threefish-256 under related-key, related-tweak assumption and against at least 19 rounds in fixed-key, related-tweak setting.
- A straightforward model of the differential behaviour of the Mix transform together with exact computations of differential characteristics of bitwise addition and rotation is enough to get useful predictions of attack complexities for attacks using modular differentials.

Bundesamt für Sicherheit in der Informationstechnik

Thank you for your attention!

 J.P. Aumasson, C. Calik, W. Meier, O. Özen, R. Phan, K. Varici, *Improved Cryptanalysis of Skein*, Advances in Cryptology - Asiacrypt 2009

 J. Chen, K. Jia, *Improved Related-Key Boomerang Attacks on Round-Reduced Threefish-512*, Information Security - Practice and Experience, Lecture Notes in Computer Science 6047/2010, 2010, S. 1-18

 M. Daum, *Cryptanalysis of Hash Functions of the MD4 family*, PhD thesis, Ruhr-Unversität Bochum, 2005

 H. Lipmaa, J. Wallén, P. Dumas, *On the Additive Differential Probability of Exclusive-Or*, Fast Software Encryption 2004

S. Liu, L. Wang, Z. Gong, *Improved Related-Key Boomerang Distinguishing Attack of Threefish-256*, IACR e-print report 323/2011