A practical distinguisher on the full Skyscraper permutation

Antoine Bak

antoine.bak@inria.fr

Inria, Paris

DGA, Paris

Abstract

Skyscraper is a cryptographic permutation published in TCHES 2025, optimized for use in proof systems such as $\mathcal{P}\mathfrak{lon}\mathcal{K}$. This primitive is based on a 10-round Feistel network combining x^2 monomials and lookup-based functions to achieve competitive plain performances and efficiency in proof systems supporting lookups. In terms of security, the x^2 monomials are supposed to provide security against statistical attacks, while lookups are supposed to provide security against algebraic attacks.

In this note, we show that this primitive has a much lower security margin than expected. Using a rebound attack, we find practical truncated differentials on the full permutation. As a corollary, we also find a practical collision attack on the compression function based on a 9-round Skyscraper permutation, which significantly reduces the security margin of the primitive. All of these attacks have been implemented and work in practice.

1 Description of Skyscraper

Description. The Skyscraper [BGK+25] permutation is defined as a 10-round Feistel network operating on any $\mathbb{F}_q^2$, where $q = p^r \geq 2^{248}$ is a power of primes. This Feistel network uses two kinds of nonlinear operations as F-boxes. The first one is based on the x^2 power map, while the Bars F-boxes are based on split-and-lookup functions [GKL+22]. More precisely, the square steps are defined as:

$$\mathrm{Sq}_c(x_\mathrm{L}, x_\mathrm{R}) = (x_\mathrm{R} + x_\mathrm{L}^2 + c, x_\mathrm{L})$$

and the Bars step as:

$$\mathtt{FBars}_c(x_\mathrm{L}, x_\mathrm{R}) = (x_\mathrm{R} + \mathtt{Bars}(x_\mathrm{L}) + c, x_\mathrm{L})$$

where c is the round constant. The Skyscraper permutation is then defined as:

$$\begin{aligned}\mathsf{Skyscraper} = {} & \mathrm{Sq}_{c_{10}} \circ \mathrm{Sq}_{c_9} \circ \mathtt{FBars}_{c_8} \circ \mathtt{FBars}_{c_7} \\ & \circ \mathrm{Sq}_{c_6} \circ \mathrm{Sq}_{c_5} \circ \mathtt{FBars}_{c_4} \circ \mathtt{FBars}_{c_3} \circ \mathrm{Sq}_{c_2} \circ \mathrm{Sq}_{c_1} \ .\end{aligned}$$

This permutation is used for 2-to-1 compression as follows:

1. Let $(y_L, y_R) = \mathsf{Skyscraper}(x_L, x_R)$.
2. Return $y_L + x_L$.

Design rationale. The choice of a Feistel network allows the use of nonbijective functions, such as the x^2 power maps and the χ-based split-and-lookups, which would otherwise require primes such as the Goldilocks prime to be bijective [GKL+24]. Both of these nonlinear operations are quite efficient both in terms of plain implementation and constraints in proof systems. The x^2 maps are supposed to provide security against statistical attacks (x^2 is a perfect nonlinear function) and the `Bars` layer provides security against algebraic attacks as it has maximal degree over $\mathbb{F}_q$.

Designer's security analysis. The designers claim a security level of 124 bit against collision attacks for compression functions and sponge hash functions based on the permutation. Their security analysis concluded that 2 square rounds and 3 `Bars` rounds are sufficient for this security level. They added 4 square rounds and 1 `Bars` round as a security margin.

2 Description of the attack

Our attack exploits the weak differential properties of the `Bars` layer, which allow some high probability differentials from the middle rounds to the external ones. We use the inbound phase to get control over the differentials in the input and output of the two middle x^2 rounds. Then, the external x^2 rounds have some probability 1 truncated differentials as they are 2-round Feistels. Our attack is summarized Figure 1.

2.1 Attack outline

Our attack is a rebound attack [MRST09] starting from the middle x^2 layers. As this layer has a very simple algebraic structure, we can find pairs of internal states $(x_\mathrm{L}, x_\mathrm{R}), (x'_\mathrm{L}, x'_\mathrm{R})$ matching any differential (β, α) in the input and (α', β') in the output in $\mathcal{O}(1)$ field operations. As the `Bars` layers have very weak statistical properties, we can choose characteristics of the form $(\beta, \alpha) \rightsquigarrow (\Delta_\mathrm{in}, 0)$ in the input and $(\alpha', \beta') \rightsquigarrow (0, \Delta_\mathrm{out})$ in the output which have high probability. We give more details for the choice of these characteristics further below.

Finally, the zero differential allows us to activate only the second x^2 box in both the input and output x^2 steps, leading the truncated differential characteristics $(\Delta_\mathrm{in}, 0) \rightsquigarrow (\Delta_\mathrm{in}, ?)$ and $(0, \Delta_\mathrm{out}) \rightsquigarrow (?, \Delta_\mathrm{out})$ to propagate with probability 1. Our attack strategy is summarized in Figure 1.

Note that removing the last Sq round and taking $\Delta_\mathrm{out} = -\Delta_\mathrm{in}$ provides a truncated differential characteristic of the form $(\Delta_\mathrm{in}, ?) \rightsquigarrow (-\Delta_\mathrm{in}, 0)$ on the Skyscraper permutation reduced to 9 rounds (the wire swap in the Feistel network is also removed). This in turn provides a collision on the compression function described in [BGK+25]. Hence our work shows that when used in compression mode, the Skyscraper permutation has no security margin.

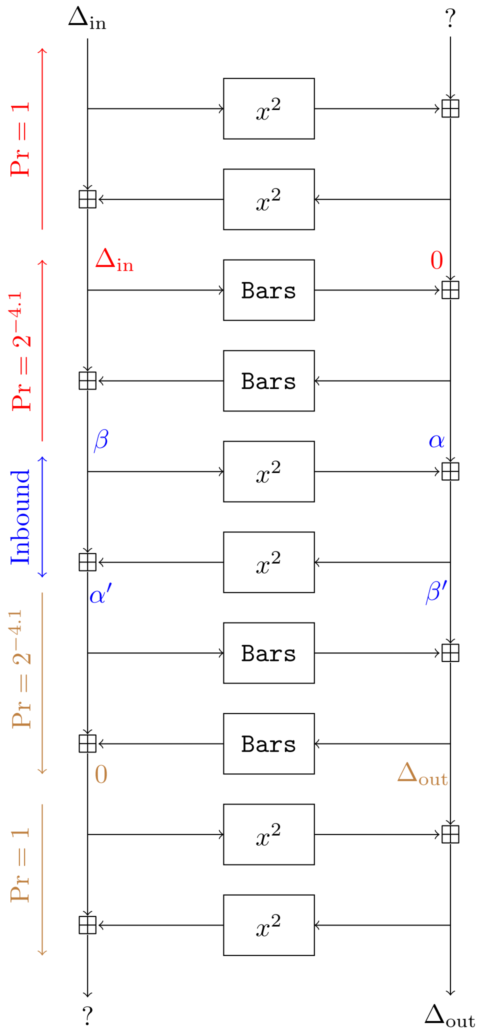

Figure 1: Rebound attack on the Skyscraper permutation

2.2 Choice of the differential characteristics

On the input side, we need a characteristic $(\beta, \alpha) \rightsquigarrow (\Delta_{\text{in}}, 0)$ through the inverse of a 2-round Feistel. Using a path with the differential $\alpha \rightsquigarrow \gamma$ on the first `Bars` and $\beta - \gamma \rightsquigarrow \alpha$ on the second `Bars`, we get the characteristic we want with probability at least

$$\Pr(\alpha \rightsquigarrow \gamma) \cdot \Pr(\beta - \gamma \rightsquigarrow \alpha) \ .$$

In the end we get $\Delta_{\text{in}} = \beta - \gamma$.

On the output side, we need a characteristic $(\alpha', \beta') \rightsquigarrow (0, \Delta_{\text{out}})$ through a 2-round Feistel. Using a path with the differential $\alpha' \rightsquigarrow \gamma'$ on the first `Bars` and $\beta' + \gamma' \rightsquigarrow -\alpha'$ on the second `Bars`, we get the characteristic we want with probability at least

$$\Pr(\alpha' \rightsquigarrow \gamma') \cdot \Pr(\beta' + \gamma' \rightsquigarrow -\alpha') \ .$$

In the end we get $\Delta_{\text{out}} = \beta' + \gamma'$.

Differential properties of `Bars`. By studying experimentally the differential properties of the shifted χ function [Dae95] `Bar` as an integer function, we get that the differentials $\pm 2^i \rightsquigarrow \pm 2^{i+1}$ where $i \in \{0, 1, 2, 3, 4\}$ have the highest probability, that is $62/256 \sim 2^{-2.046}$. Taking into account the circular shift of the bytes in `Bars`, we get differentials

$$\pm 2^{i+8j} \rightsquigarrow \pm 2^{i+8j+129}$$

and

$$\pm 2^{i+8j+128} \rightsquigarrow \pm 2^{i+8j+1}$$

with probability at least $62/256 \sim 2^{-2.046}$ when $i \in \{0, 1, 2, 3, 4\}, 0 \leq j \leq 15$.

Using this knowledge, we can let $\gamma = \alpha \cdot 2^{129}$, $\beta = 5\alpha \cdot 2^{127}$ for the input and $\gamma' = \alpha' \cdot 2^{129}$, $\beta' = -5\alpha' \cdot 2^{127}$ for the output, where $\alpha, \alpha' = \pm 2^{i+8 \cdot j}, i \in \{1, 2, 3, 4\}, 0 \leq j \leq 15$. This way, the differentials propagate in the outbound phase with probability at least $(62/256)^4 \sim 2^{-8.19}$. This gives $\Delta_{\text{in}} = \alpha \cdot 2^{127}$ and $\Delta_{\text{out}} = -\alpha' \cdot 2^{127}$.

2.3 Results

This attack provides a truncated differential using on average $2^{8.19}$ evaluations of the full permutation. We implemented this attack[1] on an instance defined over the 254-bit prime p_{BLS} instance and it provides several truncated differentials in practical time.

For the collision attack on the 9-round compression function, we have to restrict ourselves to the case where $\alpha = \alpha'$. In particular, the characteristics we highlight in the last section may not be sufficient to have one conforming pair (we have 2^6 such α and each of them provides a collision with probability $2^{-8.19}$). By taking random round constants and running our attack, we observe that our attack results in a collision on the 9-round compression function for more than 1/5 of the choices of constants.

We leave as a future work the study of clustering effects in the propagation of differentials through `Bars`, and using other differential characteristics to improve the success probability of the collision attack on the 9-round compression function.

Acknowledgements

This work is funded in part by the ERC grant ReSCALE (number 101041545), and by the French DGA. We also thank Léo Perrin for proof-reading a first draft of this note.

[1] https://github.com/AntoineBak/SkyScraperCryptanalysis.

References

[BGK$^+$25] Clémence Bouvier, Lorenzo Grassi, Dmitry Khovratovich, Katharina Koschatko, Christian Rechberger, Fabian Schmid, and Markus Schofnegger. Skyscraper: Fast hashing on big primes. Cryptology ePrint Archive, Paper 2025/058, 2025.

[Dae95] Joan Daemen. *Cipher and hash function design strategies based on linear and differential cryptanalysis.* PhD thesis, Doctoral Dissertation, March 1995, KU Leuven, 1995.

[GKL$^+$22] Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, Markus Schofnegger, and Roman Walch. Reinforced concrete: a fast hash function for verifiable computation. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 1323–1335, 2022.

[GKL$^+$24] Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, Markus Schofnegger, and Roman Walch. Monolith: Circuit-friendly hash functions with new nonlinear layers for fast and constant-time implementations. *IACR Transactions on Symmetric Cryptology*, 2024(3):44–83, 2024.

[MRST09] Florian Mendel, Christian Rechberger, Martin Schläffer, and Søren S Thomsen. The rebound attack: Cryptanalysis of reduced whirlpool and grøstl. In *Fast Software Encryption: 16th International Workshop, FSE 2009 Leuven, Belgium, February 22-25, 2009 Revised Selected Papers*, pages 260–276. Springer, 2009.