Twelve-round KECCAK for secure hashing

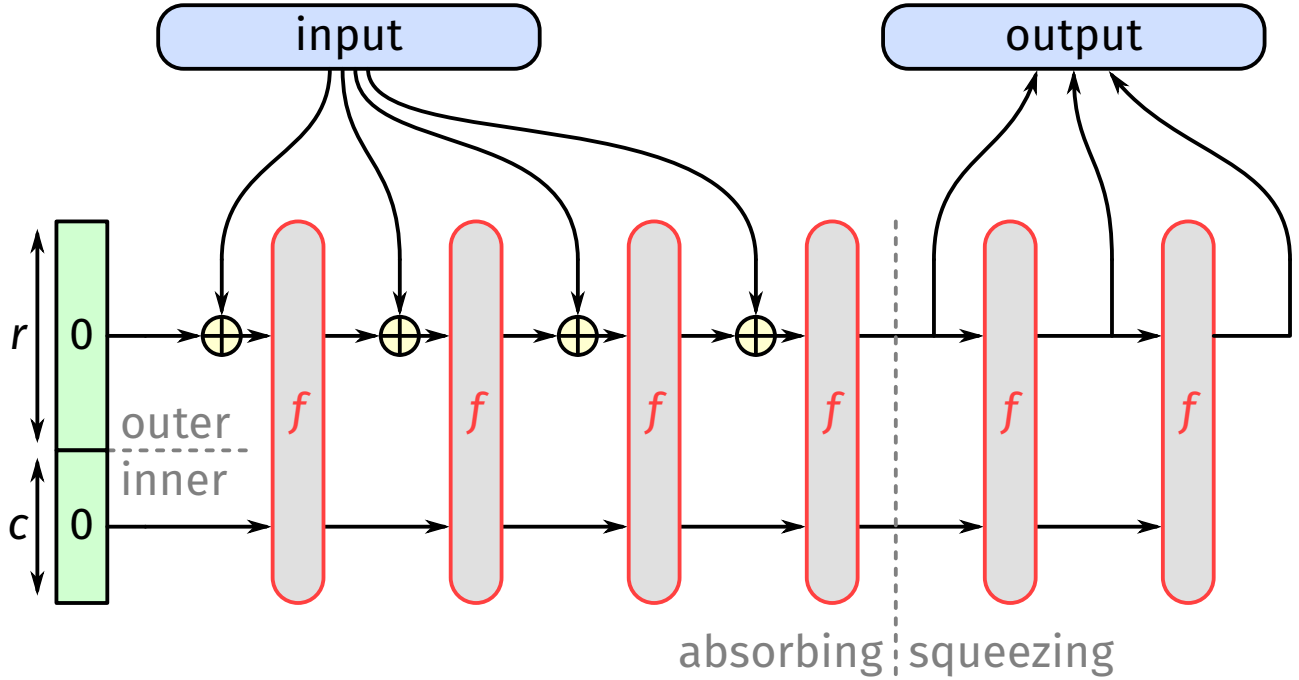
Guido BERTONI[1] Joan DAEMEN[2]
Michaël PEETERS[3] Gilles VAN ASSCHE[3]

[1]Security Pattern, Italy
[2]Radboud University, The Netherlands
[3]STMicroelectronics, Belgium

NIST 4th PQC Standardization Conference
Tuesday, November 29, 2022

Outline

The KECCAK sponge function in PQC



Sponge function on top of KECCAK-$f[1600]$, with

- $r + c = 1600$ bits
- KECCAK-$f[1600]$ = KECCAK-$p[1600, n_r = 24]$

NIST FIPS 202

- Four drop-in replacements to SHA-2
- Two *extendable output functions* (XOF)

XOF	**SHA-2 drop-in replacements**
KECCAK$[c = 256](M\|\|11\|\|11)$	
	first 224 bits of KECCAK$[c = 448](M\|\|01)$
KECCAK$[c = 512](M\|\|11\|\|11)$	first 256 bits of KECCAK$[c = 512](M\|\|01)$
	first 384 bits of KECCAK$[c = 768](M\|\|01)$
	first 512 bits of KECCAK$[c = 1024](M\|\|01)$
SHAKE128 and **SHAKE256**	**SHA3-224** to **SHA3-512**

- Toolbox for building other functions, including KECCAK-$p[1600, n_r]$

NIST SP 800-185

Customized SHAKE (**cSHAKE**)

- $H(x) = \text{cSHAKE}(x, \text{name}, \text{customization string})$
- E.g., $\text{cSHAKE128}(x, N, S) = \text{KECCAK}[c = 256](\text{encode}(N, S)||x||00)$
- $\text{cSHAKE128}(x, N, S) \triangleq \text{SHAKE128}$ when $N = S = \text{“”}$

Based on cSHAKE:

- KMAC
- TupleHash
- ParallelHash

NIST SP 800-185

Customized SHAKE (**cSHAKE**)

- $H(x) = \text{cSHAKE}(x, \text{name}, \text{customization string})$
- E.g., $\text{cSHAKE128}(x, N, S) = \text{KECCAK}[c = 256](\text{encode}(N, S)||x||00)$
- $\text{cSHAKE128}(x, N, S) \triangleq \text{SHAKE128}$ when $N = S = \text{“”}$

Based on cSHAKE:

- KMAC
- TupleHash
- ParallelHash

Security assurance of a primitive

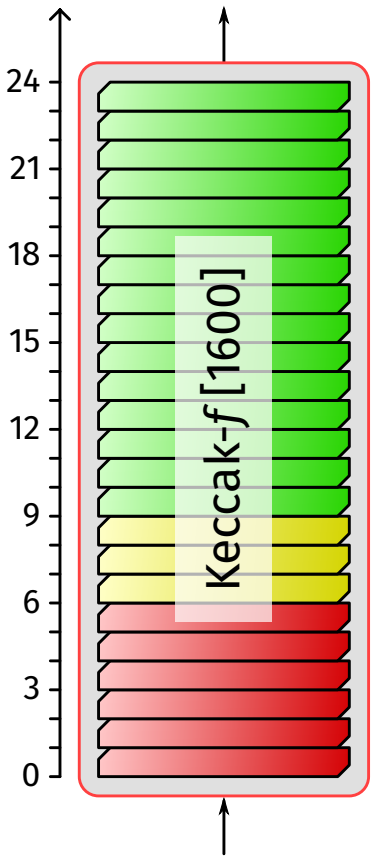
... is based on attacks on **reduced-round** versions!

Example: AES-128 has 10 rounds

- best attacks break 6 rounds (1998) to 7 rounds (a few years later)
  $\Rightarrow$ still 3 rounds of margin against progress in cryptanalysis
- 24 years of cryptanalysis since 1998
  $\Rightarrow$ progress in cryptanalysis decreased over time

$\Rightarrow$ KECCAK is in a comparable situation.

Status of KECCAK cryptanalysis



- Preimage attacks up to 4 rounds
  [He et al., ToSC 2021] [Wang et al., IACR ePrint 2022/977]
- Collision attacks up to 6 rounds
  [Song et al., CRYPTO 2017] [Guo et al., ASIACRYPT 2022]
- Structural distinguishers
  - 7 rounds (practical time)
    [Huang et al., EUROCRYPT 2017]
  - 8 rounds (2^{122} time)
    [Huang et al., IEICE 2019]
  - 9 rounds (2^{64} time) – SymSum
    [Suryawanshi et al., AFRICACRYPT 2020]
- Lots of third-party cryptanalysis available at:
  `https://keccak.team/third_party.html`

What is SymSum?

A SymSum structural distinguisher produces:

- a set S of self-symmetric input strings, i.e., $a||a||b||b||c||c||\ldots$, with $|a| = |b| = |c| = 32$ bits,
- such that

$$\bigoplus_{m \in S} H(m) \quad \text{is self-symmetric}$$

[Saha et al., ToSC 2017] [Suryawanshi et al., AFRICACRYPT 2020]

Preimage attacks

- 2 rounds

Capacity	Output	Time	Reference
160	80	Practical	[Morawiecki, Crunchy contest, 2011]
512	256	2^{33}	[Naya-Plasencia et al., Indocrypt 2011]
768	384	2^{89}	[Kumar et al., Indocrypt 2018]
768	384	2^{28}	[Le et al., ePrint 2022/788]
1024	512	2^{252}	[Le et al., ePrint 2022/788]

- 3 rounds
- 4 rounds

Preimage attacks

- 2 rounds
- 3 rounds

Capacity	Output	Time	Reference
160	80	Practical	[Guo and Liu, Crunchy contest, 2016]
512	256	2^{150}	[Li et al., ToSC 2017]
512	256	2^{81}	[Li et al., Eurocrypt 2019]
512	256	2^{65}	[Lin et al., ToSC 2021]
576	512	2^{506}	[Morawiecki et al., FSE 2013]
1024	512	2^{440}	[Liu et al., ePrint 2020/346]
1024	512	2^{426}	[Le et al., ePrint 2022/788]

- 4 rounds

Preimage attacks

- 2 rounds
- 3 rounds
- 4 rounds

Capacity	Output	Time	Reference
160	80	Practical	[Liu and Guo, Crunchy contest, 2016]
256	128	2^{106}	[Guo et al., Asiacrypt 2016]
448	224	2^{218}	[Wang et al., ePrint 2022/977]
448	224	Q 2^{110}	[Wang et al., ePrint 2022/977]
512	256	2^{239}	[Li et al., Eurocrypt 2019]
512	256	2^{218}	[He et al., ToSC 2021]
512	256	Q 2^{128}	[Wang et al., ePrint 2022/013]
768	384	2^{371}	[Rajasree, Indocrypt 2019]
768	384	2^{366}	[Liu et al., ePrint 2020/346]
1024	512	Q 2^{255}	[Wang et al., ePrint 2022/013]

Collision attacks

- 4 rounds

Capacity	Output	Time	Reference
160	160	Practical	[Dinur et al., Crunchy contest, 2011]
512	256	Practical	[Dinur et al., FSE 2012]
≤ 640	any	Practical	[Kölbl et al., IMA Int. Conf., 2013]
768	384	2^{147}	[Dinur et al., FSE 2013]
768	384	2^{59}	[Huang et al., ToSC 2022]

- 5 rounds
- 6 rounds

Collision attacks

- 4 rounds
- 5 rounds

Capacity	Output	Time	Reference
160	160	Practical	[Qiao et al., Crunchy contest, 2016]
256	256	Practical	[Qiao et al., Eurocrypt 2017]
448	224	2^{101}	[Qiao et al., Eurocrypt 2017]
448	224	Practical	[Song et al., Crypto 2017]
512	256	2^{115}	[Dinur et al., FSE 2013]
512	256	Practical	[Guo et al., JoC 2020]

- 6 rounds

Collision attacks

- 4 rounds
- 5 rounds
- 6 rounds

Capacity	Output	Time	Reference
160	160	2^{70}	[Qiao et al., Eurocrypt 2017]
160	160	2^{50}	[Song et al., Crypto 2017]
256	256	2^{123}	[Guo et al., Asiacrypt 2022]
256	256	Q $2^{67}/\sqrt{S}$	[Guo et al., Asiacrypt 2022]
448	224	Q $2^{97}/\sqrt{S}$	[Guo et al., Asiacrypt 2022]
512	256	Q $2^{104}/\sqrt{S}$	[Guo et al., Asiacrypt 2022]

TurboSHAKE

Goal

Define a XOF based on KECCAK-$p[1600, n_r = \mathbf{12}]$

Requirements:

- Suitable for PQC candidates
- Minimize the number of instances!
  - one for $c = 256$ + one for $c = 512$?
  - easier domain separation
- Multi-string input – $H(A; B; C)$ vs $H(A||B||C)$?
- Parallelism for long inputs?
- ... ?

Conclusions

- Extensive cryptanalysis on KECCAK
- $\Rightarrow$ KECCAK with 12 rounds
  - has plenty of safety margin
  - yields a better performance/security trade-off
- TurboSHAKE to be defined

Thanks for your attention!

Conclusions

- Extensive cryptanalysis on KECCAK
- $\Rightarrow$ KECCAK with 12 rounds
  - has plenty of safety margin
  - yields a better performance/security trade-off
- TurboSHAKE to be defined

Thanks for your attention!

Conclusions

- Extensive cryptanalysis on KECCAK
- $\Rightarrow$ KECCAK with 12 rounds
  - has plenty of safety margin
  - yields a better performance/security trade-off
- TurboSHAKE to be defined

Thanks for your attention!

Conclusions

- Extensive cryptanalysis on KECCAK
- $\Rightarrow$ KECCAK with 12 rounds
  - has plenty of safety margin
  - yields a better performance/security trade-off
- TurboSHAKE to be defined

Thanks for your attention!