Variants of Sponge-like Construction

Yuji Suga
Sponge construction

• Proposed by Bertoni et al. [1]
  – Simple iterated construction

• Keccak by Bertoni et al.[SHA-3(2008)]
  – Quark by Aumasson et al.[CHES2010]
  – Photon by Guo et al.[CRYPTO2011]
  – Spongent by Bogdanov et al.[CHES2011]

[1] G. Bertoni, J. Daemen, M. Peeters and G. Van Assche, 
Sponge construction

absorbing | squeezing

© Keccak Team
http://sponge.noekeon.org/
Sponge

Absorbing -then- Squeezing
Motivation

Why only Sponge?
Motivation

• To apply alternatives of “Sponge”, we can design new constructions.

• There are many house-cleaning goods.
Mop

Absorbing -then- Squeezing
Mop with Squeezer

Absorbing -then- Squeezing
Mop with Squeezer

Absorbing -then- Squeezing w/ Rotation
Sponge construction

\[ \begin{array}{c}
  \begin{array}{c}
    r \\
    c
  \end{array} \\
  \begin{array}{c}
    0 \\
    0
  \end{array}
\end{array} \quad \begin{array}{c}
  f \\
  f \\
  \ldots \quad f \\
  f \\
  \ldots
\end{array} \quad \begin{array}{c}
  p_0 \\
  p_1 \\
  p_i \quad z_0 \\
  z_1
\end{array} \quad \begin{array}{c}
  \text{absorbing} \\
  \text{squeezing}
\end{array} \]
Mop construction

\[ \text{absorbing} \big| \text{squeezing} \quad \text{w/ Rotation} \]

\[ p_0 \quad p_1 \quad p_i \quad z_0 \quad z_1 \]

© Ketchup Team
Broom and Dustpan

Sweeping -then-
Broom construction

(Gathering up)

Sweeping

Cleaning

$p_0$

$p_1$

$p_i$

$z_0$ (1 bit)

$z_1$ (1 bit)

© Ketchup Team
Scrubbing Brush

Scrubbing -then- Scrubbing
Brush construction

Scrubbing

© Ketchup Team
Brush construction

Scrubbing  Scrubbing
Sink Plunger

Queuing -then- Picking out
Plunger construction

Queuing  Picking out

\[ p_0, p_1, p_i, p_{i-1} \]
Conclusion

• I know a sponge is the best.

• Future works
  – Window squeezer and ...
  – Kitchen items
Conclusion

• I know a sponge is the best.

• Future works
  – Window squeezer and ...
  – Kitchen items

Join us!

© Ketchup Team