

Trzydziestu kandydatów do SHA-3

<http://ipsec.pl/kryptografia/2008/trzydziestu-kandydatow-do-sha-3.html>

{

{W piątek 31 października upłynął termin zgłaszania kandydatów do ogłoszonego przez [ja href="http://csrc.nist.gov/">](http://csrc.nist.gov/) konkursu na nowy standard funkcji skrótu o roboczej nazwie [ja href="http://csrc.nist.gov/groups/ST/hash/sha-3/index.html"](http://csrc.nist.gov/groups/ST/hash/sha-3/index.html) SHA-3. Do konkursu spłynęło ponoć prawie 30 propozycji od zespołów z całego świata.

{Konkurs SHA-3 ma być podobny do procesu, w jakim wyłoniono standard AES - tam zwycięzca został holenderski Rijndael. Celem konkursu SHA-3 jest wyłonienie funkcji skrótu na najbliższe dekady. Jego główna motywacja są potencjalne ataki kryptoanalityczne na dotychczasowy standard SHA-1. W odpowiedzi na nie NIST stworzył rodzinę skrótów SHA-2, których architektura jest jednak bardzo podobna do SHA-1.

{Według NIST nie ma podstaw do twierdzenia, że funkcje SHA-2 mogą być w nadchodzących latach podatne na ataki, ale fakt że od bezpieczeństwa funkcji skrótu zależy długoterminowe bezpieczeństwo np. podpisu elektronicznego jest wystarczającym powodem by w perspektywie kilku lat zastąpić SHA-2 nowym standardem wyłonionym na drodze publicznego konkursu.

- [ja href="http://csrc.nist.gov/groups/ST/hash/sha-3/index.html"](http://csrc.nist.gov/groups/ST/hash/sha-3/index.html) Więcej informacji o konkursie na stronie NIST - Cryptographic Hash Algorithm Competition [ja](#)

{Nazwy większości zgłoszonych algorytmów można znaleźć na stronie [ja href="http://ehash.iaik.tugraz.at/wiki/The_SHA3_Zoo"](http://ehash.iaik.tugraz.at/wiki/The_SHA3_Zoo) > SHA-3 Zoo < /a > . *W miarę publikacji zgłoszonych algorytmów przez NIST lub przez autorów wyników testów* [ahref = "http : //bench.cr.yp.to/ebash.html"](http://bench.cr.yp.to/ebash.html) > eBATS < /a > . *Obecnie astronomie SHA - 3 Zoo wymienia następujące algorytmy :*

{[ja href="http://www.131002.net/papers.html"](http://www.131002.net/papers.html) BLAKE [ja](#)- autorzy Jean-Philippe Aumasson, Luca Henzen, Willi Meier, Raphael C.-W. Phan

{Blue Midnight Wish - autorzy Danilo Gligoroski, Vlastimil Klima, Svein Johan Knapskog, Mohamed El-Hadedy, Jørn Amundsen, Stig Frode Mjølsnes

{[ja href="http://ehash.iaik.tugraz.at/uploads/3/37/BoolePaper.pdf"](http://ehash.iaik.tugraz.at/uploads/3/37/BoolePaper.pdf) Boole [ja](#)- autor Greg Rose

{[ja href="http://cubehash.cr.yp.to/"](http://cubehash.cr.yp.to/) CubeHash [ja](#)- autor Dan Bernstein

{Edon-R - autorzy Danilo Gligoroski, Rune Steinsmo Ødegård, Marija Mihova, Svein Johan Knapskog, Ljupco Kocarev, Aleš Drápal

{[ja href="http://www.enrupt.com/"](http://www.enrupt.com/) EnRUPT [ja](#)- autorzy Sean O'Neil, Karsten Nohl, Luca Henzen

{[ja href="http://www.math.jmu.edu/~martin/essence/"](http://www.math.jmu.edu/~martin/essence/) ESSENCE [ja](#)- autor Jason Worth Martin

{[ja href="http://www.groestl.info/"](http://www.groestl.info/) Groestl [ja](#)- autorzy Praveen Gauravaram, Lars R. Knudsen, Krystian Matusiewicz, Florian Mendel, Christian Rechberger, Martin Schläffer, Søren S. Thomsen

{[ja href="http://keccak.noekeon.org/"](http://keccak.noekeon.org/) Keccak [ja](#)- autorzy Guido Bertoni, Joan Daemen, Michaël Peeters and Gilles Van Assche

{[ja href="http://burtleburtle.net/bob/crypto/maraca/nist/"](http://burtleburtle.net/bob/crypto/maraca/nist/) Maraca [ja](#)- autor Robert J. Jenkins Jr.

{[ja href="http://registercsp.nets.co.kr/hash_competition.htm"](http://registercsp.nets.co.kr/hash_competition.htm) > MCSSHA - 3 < /a > - autor Mikhail Maslennikov { < ahref = "http : //groups.csail.mit.edu/cis/md6/" > MD6 < /a > - autorzy Ron Rivest, Benjamin Agre, Daniel V. Bailey, Christopher Crutchfield, Yevgeniy Dodis, Kermin

{ja href="http://inf.ugd.edu.mk/images/stories/file/Mileva/Nasha.htm" ;NaSHA i/a;- autorzy Smile Markovski, Aleksandra Mileva

{ja href="http://geoffrey.park.googlepages.com/home" ;NKS2D i/a;- autor Geoffrey Park

{Ponic - autor Peter Schmidt-Nielsen

{ja href="http://www.allicient.co.uk/files/sgail/" ;Sgàil i/a;- autor Peter Maxwell

{ja href="http://www.schneier.com/skein.html" ;Skein i/a;- autorzy Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, Jesse Walker

{ja href="http://www.washburnresearch.org/cryptography/index.htm" ;WaMM i/a;- autor John Washburn