

NIST's search for the super hash – just five candidates left in SHA-3 final

Written by ph0bYx

Saturday, 11 December 2010 22:59 - Last Updated Saturday, 11 December 2010 23:00

source: H-Online.com

The National Institute of Standards and Technology (NIST)'s [SHA-3](#) competition is entering its final round with five candidates – BLAKE, Grøstl, JH, Keccak and Skein – remaining. Europe's performance in the US agency's selection process has been conspicuously good.

The competition is aimed at finding a new [standard hashing algorithm](#) (SHA) for generating the next generation of secure cryptographic hashes. A hash is a kind of digital fingerprint for data and is essential for online authentication procedures and for digital signatures. Two years ago, with [SHA-1](#) no longer

considered secure (see:

[Hash cracked: The consequences of the successful attacks on SHA-1](#)

) and the successor algorithm

[SHA-2](#)

also under a cloud due to its strong similarity to SHA-1, the standardisation organisation launched a competition to

[design](#)

SHA-3. Of the remaining candidates, only BLAKE and Skein are heavily indebted to SHA-2 – the others all differ fundamentally from the current algorithm.

As well as security, a key criterion for selection is performance. Cryptologist Ron 'The R in RSA' Rivest [withdrew](#) his MD6 process – it was highly-rated but conspicuously sluggish. However the committee has not simply selected the fastest algorithms. It's clearly important that the algorithm has a clear round structure, which achieves a balance between performance and security over the number of iterations.

It's interesting that three of the five finalists have their roots in Europe. [BLAKE](#) originates in Switzerland,

[Gr](#)

NIST's search for the super hash – just five candidates left in SHA-3 final

Written by ph0bYx

Saturday, 11 December 2010 22:59 - Last Updated Saturday, 11 December 2010 23:00

[østl](#)

is the product of a collaboration between Graz University of Technology and the Technical University of Denmark, and one of the key personnel in the

[Keccak](#)

team is the Belgian Joan Daemen. Hongjun Wu, the man behind

[JH](#)

, is from Singapore.

[Cryptography guru](#)

Bruce Schneier is a key player in

[Skein](#)

, which is the only US algorithm left in the competition.

It's also notable that four of the five finalists have tweaked their designs at least once since the start of the competition. All finalists now have the opportunity to carry out further tweaks – the competition rules stipulate that all entrants have until 16th January to submit proposals for changes to prepare their algorithms for the forthcoming onslaught from the international cryptographic community. The new super hash is not scheduled to be crowned until 2012.