Le NIST (représenté par William Burr, Directeur du Cryptographic Technology Group) vient de donner la liste des 5 circuits qui sont retenus après le second tour. Ce sont BLAKE, Grøstl, JH , Keccak et Skein. Ces 5 circuits sont donc qualifiés pour le troisième et dernier tour. Je rappelle l'adresse où on peut trouver l'évolution du concours :
http://csrc.nist.gov/groups/ST/hash/sha-3/
. On peut citer ici un petit extrait du courrier envoyé par William Burr :

"The selection was challenging, because we had a strong field of fourteen hash algorithms remaining in the SHA-3 competition that were very strong contenders for the hash function standard. Security was our greatest concern, and we took this very seriously, but none of these candidates was clearly broken. However, it is meaningless to discuss the security of a hash function without relating security to performance, so in reality, NIST wanted highly secure algorithms that also performed well. We preferred to be conservative about security, and in some cases did not select algorithms with exceptional performance, largely because something about them made us “nervous,” even though we knew of no clear attack against the full algorithm."