If BLAKE is selected for the final of the SHA-3 competition, BLAKE-32 and BLAKE-28 will have 14 rounds (instead of 10), and BLAKE-64 and
BLAKE-48 will have 16 rounds (instead of 14). Apart from the number of rounds, BLAKE would remain unchanged.

A revised submission package has been prepared.

This tweak is motivated by the following facts:

1/ BLAKE is fast, and often faster than SHA-2. As security has utmost priority for us, we chose an increased number of rounds so that BLAKE now has a very conservative security margin and yet in such a way that it remains faster than SHA-2 on a number of platforms.

2/ The choice of the number of rounds affects throughput but not memory nor hardware gates. As the two latter metrics are generally the limiting factors in embedded systems, more rounds will not affect BLAKE's good suitability for those systems (see e.g. XBX benchmarks).

3/ Known cryptanalysis results against reduced round versions remain valid, so the understanding of BLAKE's security continues to benefit from these public scrutiny and third party analysis.

The best attack on the (reduced) hash functions that we are aware of is a preimage attack on 2.5 rounds (both for BLAKE-32 and BLAKE-64), as reported on the SHA-3 Zoo. A high-complexity distinguisher for 7 middle rounds of the compression function of BLAKE-32 has been reported to us, but is unpublished.

Based on the software benchmarks reported on eBASH, we estimated the speed of the tweaked BLAKE-32 and BLAKE-64 by multiplying the cycles/byte counts by a factor respectively 14/10 and 16/14 (which overestimates the actual cycles/byte value, as it assumes that all computations, not only rounds, are multiplied by this factor).

As an illustration, we considered the first 7 machines on eBASH with recent results (201011*) for amd64 (64-bit) and x86 (32-bit) modes.
At the end of this email, we list for these machines the cycles/byte counts for long messages as reported on eBASH for BLAKE-32, BLAKE-32, SHA-256, and SHA-512, and we add the estimate obtained for the tweaked BLAKE.

The BLAKE team

gcc11 (Opteron, 64)
blake32 13.21 -> 18.49
blake64 9.04 -> 10.33
sha256 14.98
sha512 11.65

dragon (Xeon, 64)
blake32 7.65 -> 10.71
blake64 6.98 -> 7.98
sha256 17.33
sha512 11.82

```
katana (Core 2 Duo, 64)
blake32 10.25 -> 14.35
blake64  7.04 ->  8.05
sha256  15.34
sha512  11.73

gcc16 (Opteron, 64)
blake32 13.61 -> 19.05
blake64  9.38 -> 10.72
sha256  15.18
sha512  11.36

ranger (Phenom, 64)
blake32 11.71 -> 16.39
blake64  7.33 ->  8.38
sha256  15.06
sha512  9.92

nmih002 (Core 2 Quad, 64)
blake32 10.35 -> 14.49
blake64  8.27 ->  9.45
sha256  15.30
sha512  12.16

latour (Core 2 Quad, 64)
blake32 10.23 -> 14.32
blake64  8.31 ->  9.59
sha256  15.34
sha512  11.76

gcc11 (Opteron, 32)
blake32 14.55 -> 20.37
blake64 20.56 -> 23.50
sha256  18.44
sha512  23.50

katana (Core 2 Duo, 32)
blake32 10.51 -> 14.72
blake64 15.59 -> 17.82
sha256  17.57
sha512  50.19

gcc16 (Opteron, 32)
blake32 14.47 -> 20.26
blake64 21.28 -> 24.32
sha256  18.30
sha512  20.32

ranger (Phenom, 32)
blake32 13.34 -> 18.68
blake64 24.28 -> 27.75
sha256  14.99
sha512  21.48

nmih002 (Core 2 Quad, 32)
blake32 10.05 -> 14.07
blake64 51.48 -> 58.83
sha256  15.57
sha512  18.76

latour (Core 2 Quad, 32)
blake32 10.06 -> 14.08
blake64 12.65 -> 14.46
sha256  20.18
sha512  19.99
```

```
margaux (Core 2 Quad, 32)
blake32  9.99 -> 13.99
blake64 12.63 -> 14.43
sha256  20.21
sha512  20.02
```