Is SHA-3 too complicated?

Daniel J. Bernstein, Peter Schwabe, Gilles Van Assche

Is SHA-3 too complicated?

Daniel J. Bernstein, Peter Schwabe, Gilles Van Assche

`https://twitter.com/TweetFIPS202`
is the following self-contained C implementation of
SHA3-224 (`crypto_hash_sha3224`),
SHA3-256 (`crypto_hash_sha3256`),
SHA3-384 (`crypto_hash_sha3384`),
SHA3-512 (`crypto_hash_sha3512`),
SHAKE128 single-block (`crypto_hash_shake128`),
SHAKE256 single-block (`crypto_hash_shake256`):

Is SHA-3 too complicated?

Daniel J. Bernstein, Peter Schwabe, Gilles Van Assche

`https://twitter.com/TweetFIPS202`
is the following self-contained C implementation of
SHA3-224 (`crypto_hash_sha3224`),
SHA3-256 (`crypto_hash_sha3256`),
SHA3-384 (`crypto_hash_sha3384`),
SHA3-512 (`crypto_hash_sha3512`),
SHAKE128 single-block (`crypto_hash_shake128`),
SHAKE256 single-block (`crypto_hash_shake256`):

```c
#define FOR(i,n) for (i = 0;i < n;++i)
#define H(i,r,p,d) int crypto_hash_##i(u8 *h,const u8 *m,u64 n) { Keccak(r*8,m,n,6+25*p,h,d); return 0; }
typedef unsigned char u8;typedef unsigned long long u64;static u64 ROL(u64 a,u8 n){return(a<<n)|(a>>(64-n));}static u64 L64(const u8*x){u64
r=0,i;FOR(i,8)r|=(u64)x[i]<<8*i;return r;}static void F(u64*s){u8 x,y,j,R=1,r,n;u64 t,B[5],Y;FOR(n,24){FOR(x,5){B[x]=0;FOR(y,5)B[x]^=s[x+5*y
];}FOR(x,5){t=B[(x+4)%5]^ROL(B[(x+1)%5],1);FOR(y,5)s[x+5*y]^=t;}t=s[1];y=r=0;x=1;FOR(j,24){r+=j+1;Y=2*x+3*y;x=y;y=Y%5;Y=s[x+5*y];s[x+5*y]=
ROL(t,r%64);t=Y;}FOR(y,5){FOR(x,5)B[x]=s[x+5*y];FOR(x,5)s[x+5*y]=B[x]^(~B[(x+1)%5]&B[(x+2)%5]);}FOR(y,7)if((R=(R<<1)^(113*(R>>7)))&2)*s^=
1ULL<<((1<<y)-1);}}static void Keccak(u8 r,const u8*m,u64 n,u8 p,u8*h,u64 d){u64 s[25],i;u8 t[200];FOR(i,25)s[i]=0;while(n>=r){FOR(i,r/8)s[i
]^=L64(m+8*i);F(s);n-=r;m+=r;}FOR(i,r)t[i]=0;FOR(i,n)t[i]=m[i];t[i]=p;t[r-1]|=128;FOR(i,r/8)s[i]^=L64(t+8*i);F(s);FOR(i,d)h[i]=s[i/8]>>8*(i%
8);}H(shake128,21,1,168)H(shake256,17,1,136)H(sha3224,18,0,28)H(sha3256,17,0,32)H(sha3384,13,0,48)H(sha3512,9,0,64)
```