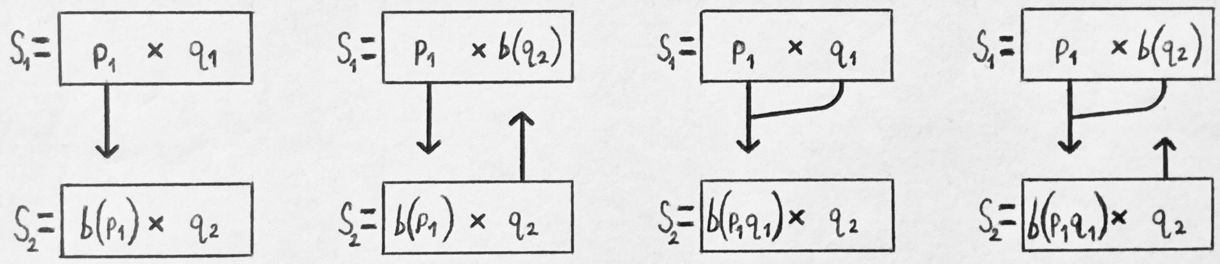
2. Primality-adjusting branded strings – As seen in early and overly-complex versions of CSC it is possible to ensure that all CSC packages consist strictly of a single semiprime or other one-way function, however, since that semiprime must sit around factored in order to reveal the user data within it, it is no different than pointing directly at a hash (deductive lossy compression) of a new list of semiprimes or one-way functions. The current version omits this unnecessary technicality but the possibility exists through primality-adjusting branded strings where semiprimes are built to hide information. —

A cryptographic prime is a long random number where search algorithms find the nearest prime and set the random number equal to that prime, adjusting only the last few digits. Without disturbing those last few digits, it is possible to brand the random number before it is prime, replacing a portion of the digits with data in base ten. Once the prime is multiplied by another the branded message is locked away securely. This branded message can be the hash of another semiprime or its factors, establishing a strong cryptographic relationship between two or more numbers. The following four are the basic linking styles of branding for semiprime pairs where **b()** represents "branded with."


$S_1 = p_1 \times q_1$
$S_2 = b(p_1) \times q_2$
$S_1 = p_1 \times b(q_2)$
$S_2 = b(p_1) \times q_2$
$S_1 = p_1 \times q_1$
$S_2 = b(p_1 q_1) \times q_2$
$S_1 = p_1 \times b(q_2)$
$S_2 = b(p_1 q_1) \times q_2$

Semiprimes open to observation are not to share factors, that would increase the sample size for cryptanalysis. It is unsafe to reveal branded factors before their unbranded links. In the first example, S_1 should be factored first if there are to be multiple events for the two-stage process ($b(p_1)$ is a key fragment of S_1.)

Primality-adjusting branded strings empower semiprime-based encryption where semiprimes need not share factors if some shared key is transformed. And repetative data would not degrade file randomness thanks to the addition involved in multiplication. Any repeating zeros for example form diagonal ribbons who are then obfuscated by the vertical digit sum.