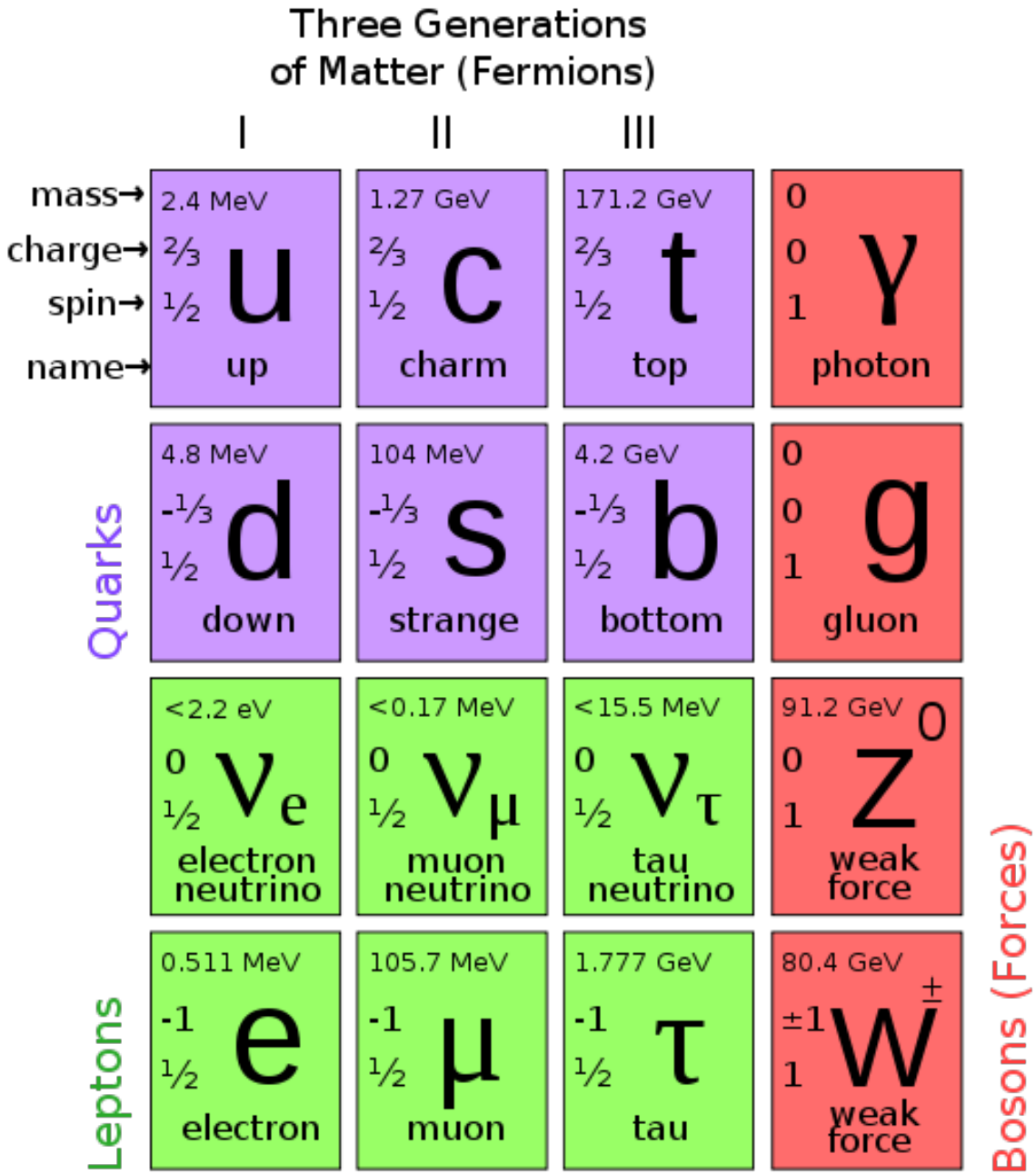
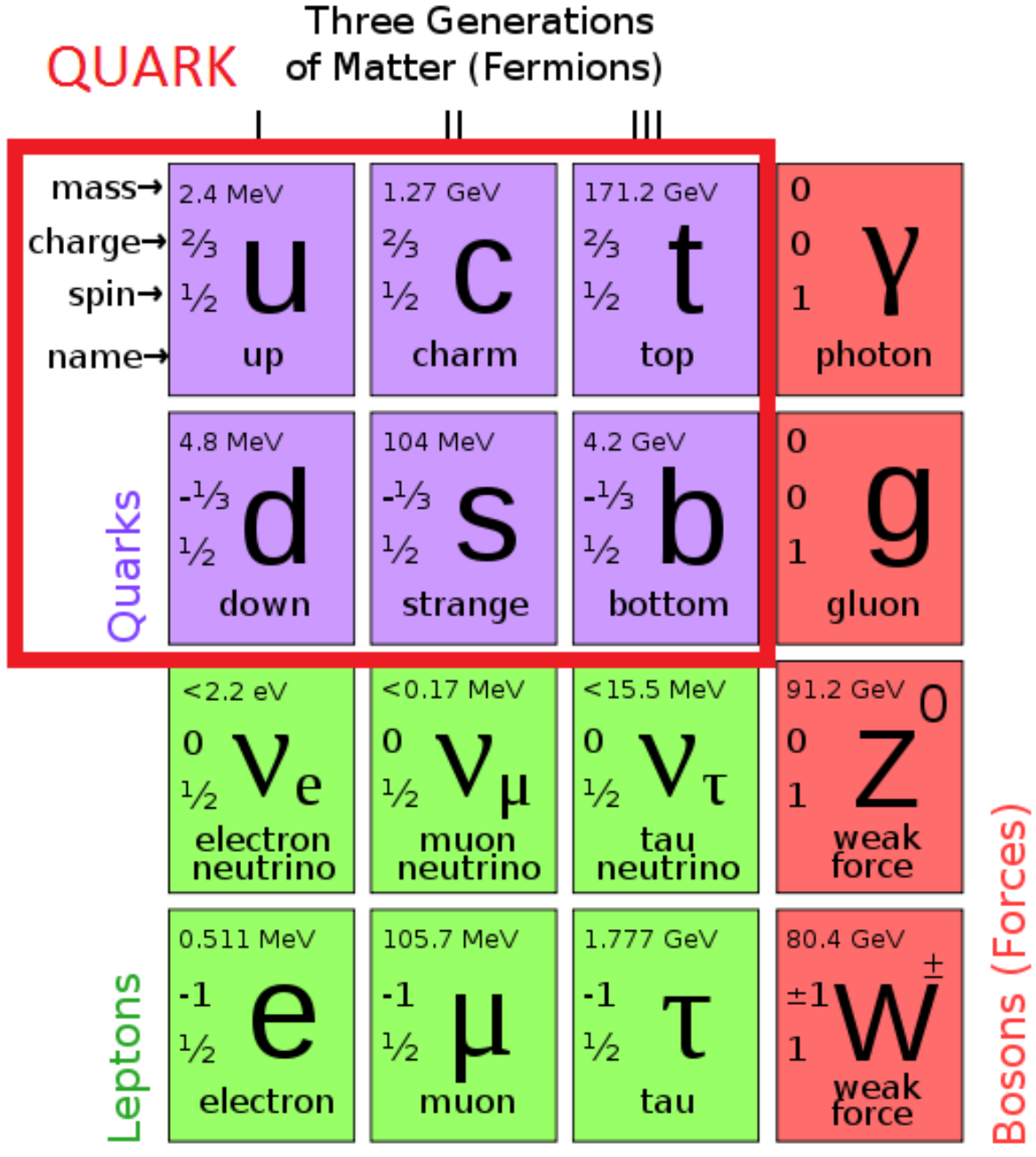
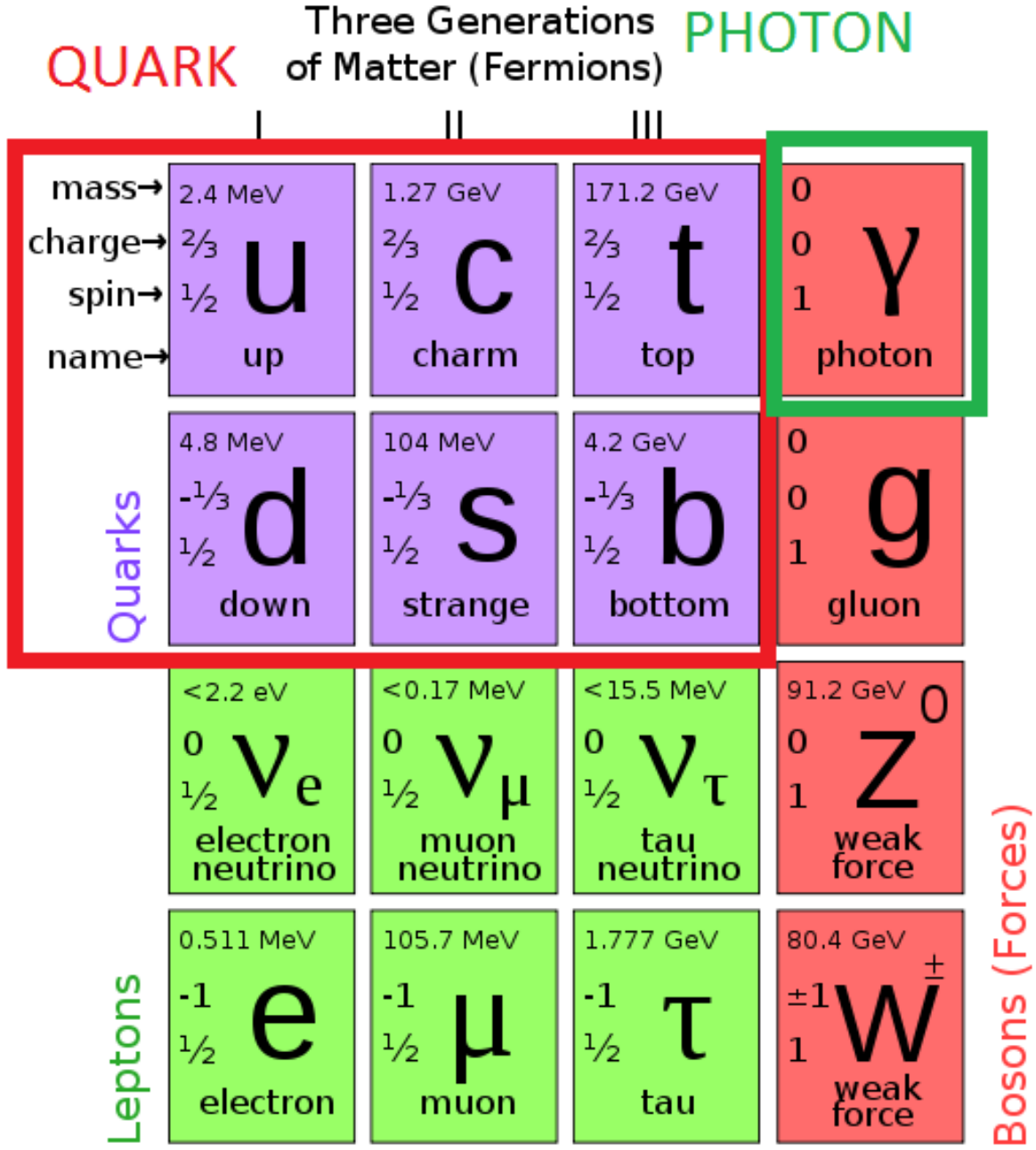
Smaller Quarks!

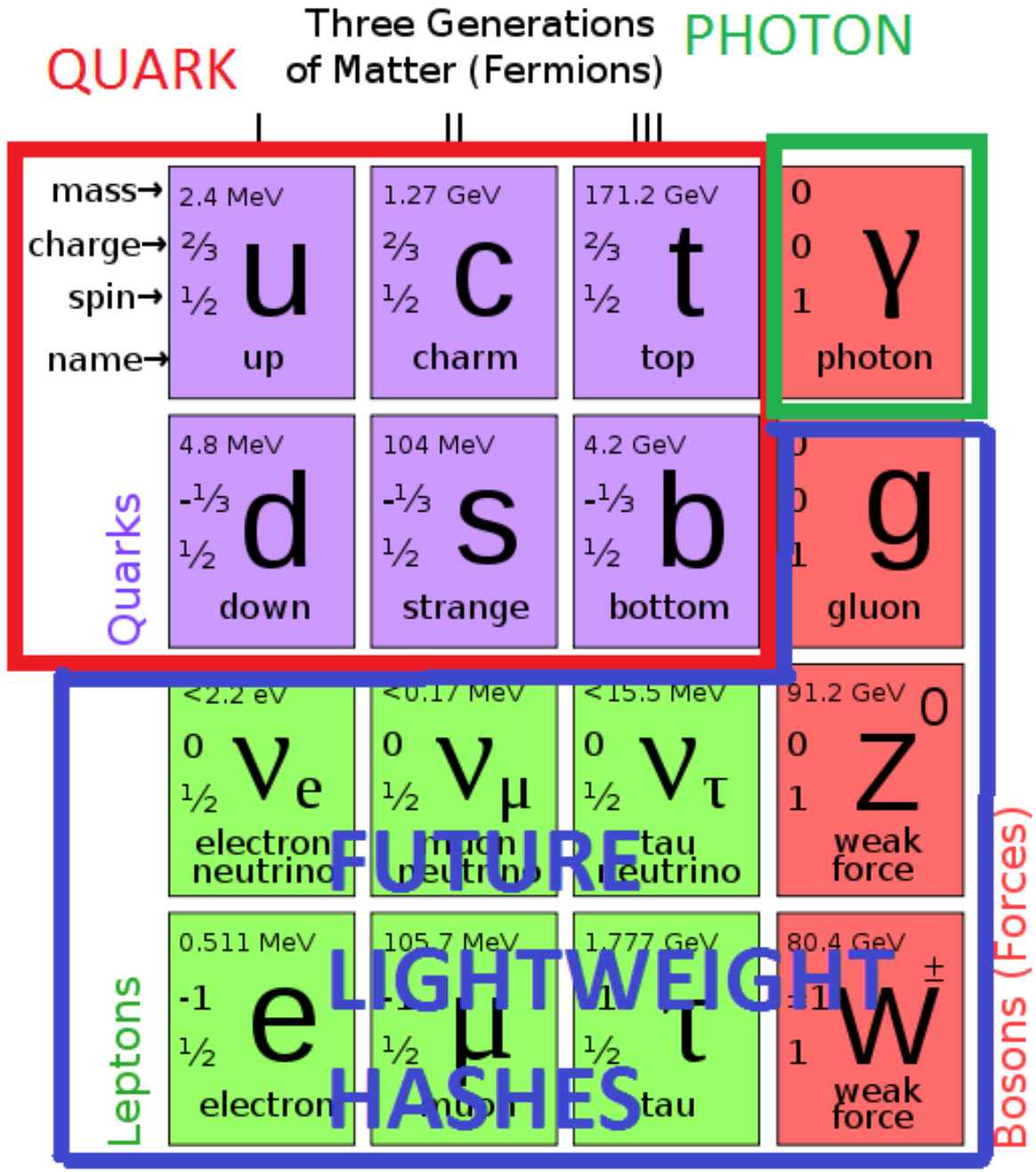
QUARK: lightweight hash function by A., Henzen, Meier, Naya-Plasencia (CHES '10)

- Based on the stream cipher Grain and the block cipher KATAN
- Sponge construction
- Implementation tradeoffs (serial/parallel)


Three Generations
of Matter (Fermions)
I
II
III
mass→
charge→
spin→
name→
2.4 MeV
⅔
½
u
up
1.27 GeV
⅔
½
c
charm
171.2 GeV
⅔
½
t
top
0
0
1
γ
photon
4.8 MeV
-⅓
½
d
down
104 MeV
-⅓
½
s
strange
4.2 GeV
-⅓
½
b
bottom
0
0
1
g
gluon
<2.2 eV
0
½
νe
electron neutrino
<0.17 MeV
0
½
νμ
muon neutrino
<15.5 MeV
0
½
ντ
tau neutrino
91.2 GeV
0
0
1
Z0
weak force
0.511 MeV
-1
½
e
electron
105.7 MeV
-1
½
μ
muon
1.777 GeV
-1
½
τ
tau
80.4 GeV
±1
1
W±
weak force
Quarks
Leptons
Bosons (Forces)


QUARK
Three Generations of Matter (Fermions)
I
II
III
mass→
charge→
spin→
name→
2.4 MeV
⅔
½
u
up
1.27 GeV
⅔
½
c
charm
171.2 GeV
⅔
½
t
top
0
0
1
γ
photon
4.8 MeV
-⅓
½
d
down
104 MeV
-⅓
½
s
strange
4.2 GeV
-⅓
½
b
bottom
0
0
1
g
gluon
Quarks
<2.2 eV
0
½
νe
electron neutrino
<0.17 MeV
0
½
νμ
muon neutrino
<15.5 MeV
0
½
ντ
tau neutrino
91.2 GeV
0
0
1
Z0
weak force
0.511 MeV
-1
½
e
electron
105.7 MeV
-1
½
μ
muon
1.777 GeV
-1
½
τ
tau
80.4 GeV
±1
1
W±
weak force
Leptons
Bosons (Forces)


QUARK
Three Generations of Matter (Fermions)
PHOTON
I
II
III
mass→
charge→
spin→
name→
2.4 MeV
⅔
½
u
up
1.27 GeV
⅔
½
c
charm
171.2 GeV
⅔
½
t
top
0
0
1
γ
photon
Quarks
4.8 MeV
-⅓
½
d
down
104 MeV
-⅓
½
s
strange
4.2 GeV
-⅓
½
b
bottom
0
0
1
g
gluon
<2.2 eV
0
½
νe
electron neutrino
<0.17 MeV
0
½
νμ
muon neutrino
<15.5 MeV
0
½
ντ
tau neutrino
91.2 GeV
0
0
1
Z0
weak force
Leptons
0.511 MeV
-1
½
e
electron
105.7 MeV
-1
½
μ
muon
1.777 GeV
-1
½
τ
tau
80.4 GeV
±1
1
W±
weak force
Bosons (Forces)


QUARK
Three Generations of Matter (Fermions)
PHOTON
I
II
III
mass→
charge→
spin→
name→
2.4 MeV
⅔
½
u
up
1.27 GeV
⅔
½
c
charm
171.2 GeV
⅔
½
t
top
0
0
1
γ
photon
Quarks
4.8 MeV
-⅓
½
d
down
104 MeV
-⅓
½
s
strange
4.2 GeV
-⅓
½
b
bottom
g
gluon
<2.2 eV
0
½
νe
electron neutrino
<0.17 MeV
0
½
νμ
muon neutrino
<15.5 MeV
0
½
ντ
tau neutrino
91.2 GeV
0
0
1
Z
weak force
FUTURE
0.511 MeV
-1
½
e
electron
105.7 MeV
-1
½
μ
muon
1.777 GeV
-1
½
τ
tau
LIGHTWEIGHT
80.4 GeV
±1
1
W
weak force
HASHES
Leptons
Bosons (Forces)

QUARK vs PHOTON

- Similar performance
- Similar simplicity
- Both are sponges
- Security of the permutation?

QUARK vs PHOTON

- Similar performance
- Similar simplicity
- Both are sponges
- Security of the permutation?
  - PHOTON: 12 rounds
  - U-QUARK: 544 rounds
  - D-QUARK: 704 rounds
  - S-QUARK: 1024 rounds

Thus, U-QUARK is 45 times more secure!

More seriously. . .

QUARK is a very conservative design

- $2\times$ the nb. of rounds of the original Grain
- Reduced parallelism for faster diffusion
- Best distinguisher on 25 % of the rounds (66 % for PHOTON)

QUARK has at least 128-bit preimage security

Can we find smaller, faster QUARK's?

SMALLER QUARK's:

64-bit preimage security:

- $c = 64$, $n = 72$, $r = 8$, 72-bit state
- ≈ 730 GE in 180 nm ASIC

96-bit preimage security:

- $c = 96$, $n = 104$, $r = 8$, 104-bit state
- ≈ 1000 GE in 180 nm ASIC

FASTER QUARK's:

128-bit preimage security:

- $3b$ rounds instead of $4b$
- $16\times$ parallelism
- 224 Mbps (instead of 84)

256-bit preimage security:

- $3b$ rounds instead of $4b$
- $32\times$ parallelism
- 1 Gbps (instead of 357)

Many more trade-offs possible. . .

Find specs, C and VHDL code on

`131002.net/quark/`