

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 →	2.4 MeV	1.27 GeV	171.2 GeV	0
charge →	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	0
spin →	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
name →	u up	c charm	t top	γ photon
Quarks	4.8 MeV	104 MeV	4.2 GeV	0
	$-\frac{1}{3}$	$-\frac{1}{3}$	$-\frac{1}{3}$	0
	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
	d down	s strange	b bottom	g gluon
Leptons	<2.2 eV	<0.17 MeV	<15.5 MeV	91.2 GeV
	0	0	0	0
	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
	ν_e electron neutrino	ν_μ muon neutrino	ν_τ tau neutrino	Z⁰ weak force
	0.511 MeV	105.7 MeV	1.777 GeV	80.4 GeV
	-1	-1	-1	± 1
	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
	e electron	μ muon	τ tau	W[±] weak force

Bosons (Forces)

QUARK Three Generations of Matter (Fermions)

	I	II	III	
mass →	2.4 MeV	1.27 GeV	171.2 GeV	0
charge →	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	0
spin →	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
name →	u up	c charm	t top	γ photon
Quarks	4.8 MeV	104 MeV	4.2 GeV	0
	$-\frac{1}{3}$	$-\frac{1}{3}$	$-\frac{1}{3}$	0
	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
	d down	s strange	b bottom	g gluon
Leptons	<2.2 eV	<0.17 MeV	<15.5 MeV	91.2 GeV ⁰
	0	0	0	0
	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
	ν_e electron neutrino	ν_μ muon neutrino	ν_τ tau neutrino	Z⁰ weak force
	0.511 MeV	105.7 MeV	1.777 GeV	80.4 GeV
	-1	-1	-1	± 1
	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
	e electron	μ muon	τ tau	W[±] weak force

Bosons (Forces)

Three Generations of Matter (Fermions) **PHOTON**

	I	II	III	
mass →	2.4 MeV	1.27 GeV	171.2 GeV	0
charge →	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	0
spin →	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
name →	u up	c charm	t top	γ photon
Quarks	4.8 MeV $-\frac{1}{3}$ $\frac{1}{2}$	104 MeV $-\frac{1}{3}$ $\frac{1}{2}$	4.2 GeV $-\frac{1}{3}$ $\frac{1}{2}$	0 0 1
	d down	s strange	b bottom	g gluon
	<2.2 eV 0 $\frac{1}{2}$	<0.17 MeV 0 $\frac{1}{2}$	<15.5 MeV 0 $\frac{1}{2}$	91.2 GeV 0 1
Leptons	ν_e electron neutrino	ν_μ muon neutrino	ν_τ tau neutrino	Z⁰ weak force
	0.511 MeV -1 $\frac{1}{2}$	105.7 MeV -1 $\frac{1}{2}$	1.777 GeV -1 $\frac{1}{2}$	80.4 GeV ± 1 1
	e electron	μ muon	τ tau	W[±] weak force
				Bosons (Forces)

Three Generations of Matter (Fermions)

QUARK PHOTON

	I	II	III	
mass →	2.4 MeV	1.27 GeV	171.2 GeV	0
charge →	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	0
spin →	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
name →	u up	c charm	t top	γ photon
	4.8 MeV	104 MeV	4.2 GeV	0
	$-\frac{1}{3}$	$-\frac{1}{3}$	$-\frac{1}{3}$	0
	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
Quarks	d down	s strange	b bottom	g gluon
	<2.2 eV	<0.17 MeV	<15.5 MeV	91.2 GeV
	0	0	0	0
	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
	ν_e electron neutrino	ν_μ muon neutrino	ν_τ tau neutrino	Z weak force
	0.511 MeV	105.7 MeV	1.777 GeV	80.4 GeV
	-1	-1	-1	±
	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
Leptons	e electron	μ muon	τ tau	W weak force

FUTURE LIGHTWEIGHT HASHES

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/