Performance

parameters	q	n = m = k	t (rounds)	s (no. of pk's)	w (seed tree)	Public Key (bytes)	Signature (bytes)
MEDS-9923	4093	14	1152	4	14	9923	9896
MEDS-13220	4093	14	192	5	20	13220	12976
MEDS-41711	4093	22	608	4	26	41711	41080
MEDS-69497	4093	22	160	5	36	55604	54736
MEDS-134180	2039	30	192	5	52	134180	132528
MEDS-167717	2039	30	112	6	66	167717	165464

advantages

- single hardness assumption: **MCE**
- simple design and arithmetic
- great flexibility in sizes
- *generic*: room for improvements!

limitations

- resulting pk's and sig's still large
- scaling to higher parameters
- needs more research on **MCE**
- *opportunity*: lots of cool research!

Performance

parameters	q	n = m = k	t (rounds)	s (no. of pk's)	w (seed tree)	**Public Key** (bytes)	**Signature** (bytes)
MEDS-9923	4093	14	1152	4	14	9923	9896
MEDS-13220	4093	14	192	5	20	13220	12976
MEDS-41711	4093	22	608	4	26	41711	41080
MEDS-69497	4093	22	160	5	36	55604	54736
MEDS-134180	2039	30	192	5	52	134180	132528
MEDS-167717	2039	30	112	6	66	167717	165464

advantages

- single hardness assumption: **MCE**
- simple design and arithmetic
- great flexibility in sizes
- *generic*: room for improvements!

limitations

- resulting pk's and sig's still large
- scaling to higher parameters
- needs more research on **MCE**
- *opportunity*: lots of cool research!

advancing

- new technique to reduce sig. size
- MEDS-13220 to **2088** bytes (-84%)
- still analysing security of technique
- *explore*: potential for new ideas!