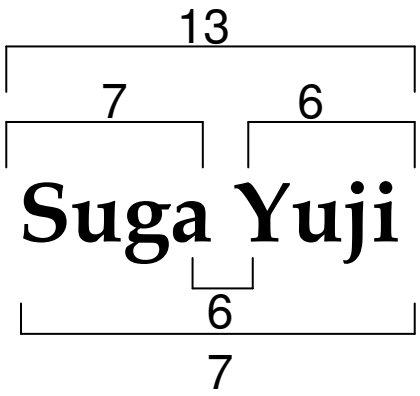
Considerations of SHA-3

Suga Yuji

Considerations of SHA-3 candidate's name



IIJ
Internet Initiative Japan

Free the SHA-3 rounds parameter

Background

- **NIST announced second round SHA-3 candidates last month.**
  - **14 candidates are selected.**
- **We did NOT know**
  why these candidates are dead/alive ?
- **So I tried to seek a borderline by only…**

My contributions

Free the SHA-3 rounds parameter

- I tried to seek a borderline by only algorithm's names.

My contributions

- I tried to seek a borderline by only algorithm's names.

- I choose the famous children's names decisional method in Japan as an evaluation tool.

How to name babies in Japan

- A majority of parents take the safe route and choose a numerically lucky name.
- Parents believe the number of strokes used in the family name and the given name must be compatible.
- There are various different styles of fortune telling for naming.

- TV stars often change their name to get lucky one.

Stroke number superstition

- We have 5 numbers from stroke number of a name.
- In alphabet, we can count it as follows:
  - Stroke number = 1 : O, I, J, S, U, L, C
    = 2 : D, G, P, Q, T, V, X, Z
    = 3 : A, B, F, H, N, R, Y, K
    = 4 : M, E, W

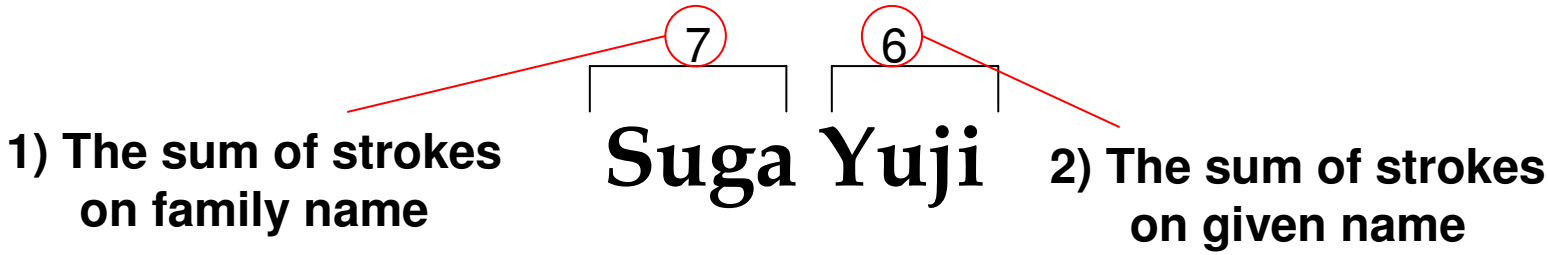
1 1 2 3 3 1 1 1

Suga Yuji

Stroke number superstition

Free the SHA-3 rounds parameter

- We have 5 numbers from stroke number of a name.



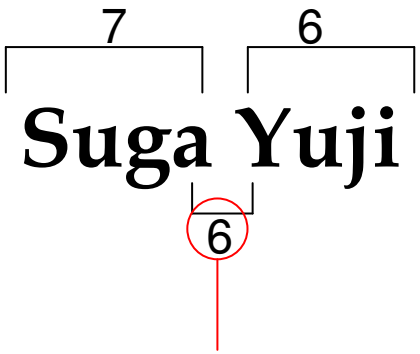
1 1 2 3 3 1 1 1

Suga Yuji

Stroke number superstition

Free the SHA-3 rounds parameter

- We have 5 numbers from stroke number of a name.



3) The last char of family name & The first char of given name

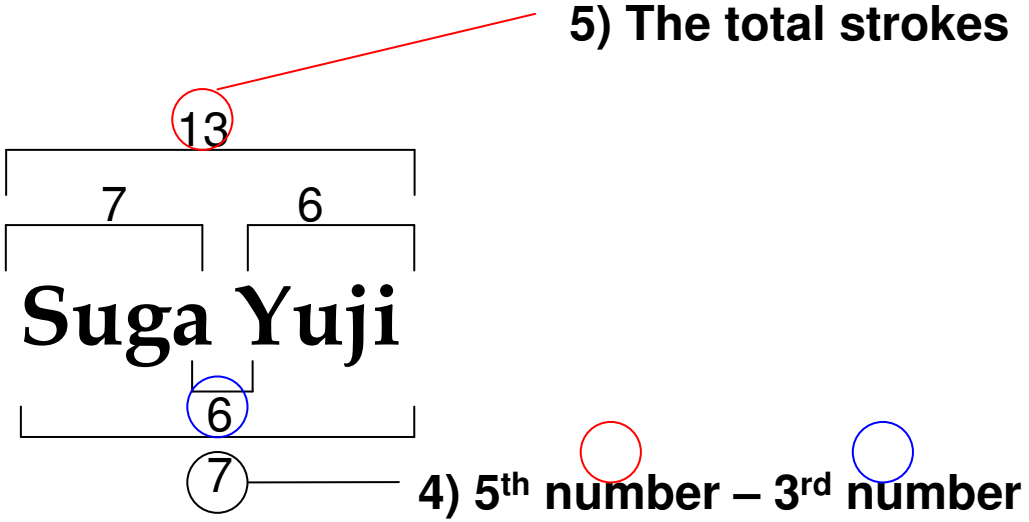
1 1 2 3 3 1 1 1

Suga Yuji

Stroke number superstition

Free the SHA-3 rounds parameter

- We have 5 numbers from stroke number of a name.



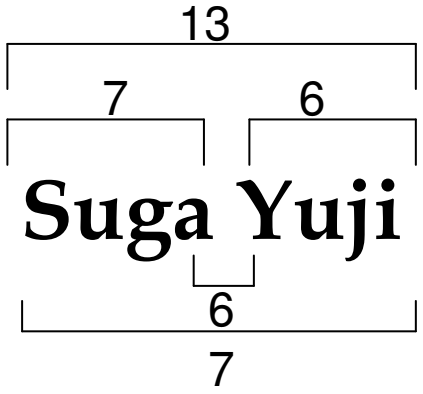
1 1 2 3 3 1 1 1

Suga Yuji

Stroke number superstition

Free the SHA-3 rounds parameter

- Check if 5 numbers are
- good : 1, 11, 16, 21, 23, …
- so-so : 3, 5, 6, 8, 13, 15, 18, 24, 25, 29, …
- bad : 7, 17, 27, 30, …
- terrible : 2, 4, 9, 10, 12, 14, 19, 20, 22, 26, …



family	given	1st	2nd	3rd	4th	5th
Suga	Yuji	7	6	6	7	13

How to split into 2 names

Free the SHA-3 rounds parameter

- Problem : We don't know a verge between family name and given name.
  - Trivial Case : CubeHash = Cube + Hash

A | urora Au | rora Aur | ora

Auro | ra Auror | a

How to split into 2 names

- **Rules :**
  - **1-1) Hyphens are omitted.**
  - **1-2) Digits are changed to words. (ex. 2 -> two)**
  - **1-3) Middle names are omitted. (ex. BMW)**

  - **2) Separate meaningful words as possible**
    - **I use spell check feature implemented in MSOffice.**
    - **Priority :**
      reasonable length > family name > given name

After applying rules 1

Original name	*Conversion (hyphens, digits)*
Blue Midnight Wish	*Blue Wish*
Dynamic SHA2	*Dynamic SHAtwo*
EDON-R	*EDON R*
Khichidi-1	*Khichidi one*
MCSSHA-3	*MCSSHA three*
MD6	*MDsix*
SHAvite-3	*SHAvite three*
TIB3	*TIBthree*

Free the SHA-3 rounds parameter

51 candidate's Japanese names

Original name	*family name*	*given name*
Abacus	*Us*	*Abac*
ARIRANG	*Ari*	*Rang*
AURORA	*Auro*	*Ra*
BLAKE	*Ke*	*Bla*
Blender	*Der*	*Blen*
Blue Midnight Wish	*Wish*	*Blue*
BOOLE	*Ole*	*Bo*
Cheetah	*Tah*	*Chee*
CHI	*Hi*	*C*
CRUNCH	*Ch*	*Crun*
CubeHash	*Hash*	*Cube*
DCH	*CH*	*D*
Dynamic SHA	*Sha*	*Dynamic*
Dynamic SHA2	*Shatwo*	*Dynamic*
ECHO	*Ho*	*Ec*

Japanese names usually consist of
a family name, followed by a given name

nese names

Free the SHA-3 rounds parameter

Original name	*family name*	*given name*
Abacus	*Us*	*Abac*
ARIRANG	*Ari*	*Rang*
AURORA	*Auro*	*Ra*
BLAKE	*Ke*	*Bla*
Blender	*Der*	*Blen*
Blue Midnight Wish	*Wish*	*Blue*
BOOLE	*Ole*	*Bo*
Cheetah	*Tah*	*Chee*
CHI	*Hi*	*C*
CRUNCH	*Ch*	*Crun*
CubeHash	*Hash*	*Cube*
DCH	*CH*	*D*
Dynamic SHA	*Sha*	*Dynamic*
Dynamic SHA2	*Shatwo*	*Dynamic*
ECHO	*Ho*	*Ec*

original name	family name	given name
ECOH	H	Eco
EDON-R	R	Edon
EnRUPT	Rupt	En
ESSENCE	Ence	ESS
FSB	B	Fs
Fugue	Gue	Fu
Grøstl	Stl	Grø
Hamsi	Si	Ham
JH	H	J
Keccak	Cak	Kec
Khichidi-1	One	Khichidi
LANE	Ne	La
Lesamnta	Lesa	Mnta
Luffa	Luf	Fa
LUX	X	Lu
MCSSHA-3	Three	Mcssha
MD6	Six	Md
MeshHash	Hash	Mesh

original name	*family name*	*given name*
NaSHA	*Sha*	*Na*
SANDstorm	*Strorm*	*Sand*
Sarmal	*Mal*	*Sar*
Sgail	*Ail*	*Sg*
Shabal	*Bal*	*Sha*
SHAMATA	*Mata*	*Sha*
SHAvite-3	*Three*	*SHAvite*
SIMD	*Md*	*Si*
Skein	*In*	*Ske*
Spectral Hash	*Hash*	*Spectral*
StreamHash	*Hash*	*Stream*
SWIFFTX	*Tx*	*Swiff*
Tangle	*Angle*	*T*
TIB3	*Three*	*Tib*
Twister	*Er*	*Twist*
Vortex	*Tex*	*Vor*
WaMM	*Mm*	*Wa*
Waterfall	*Fall*	*Water*

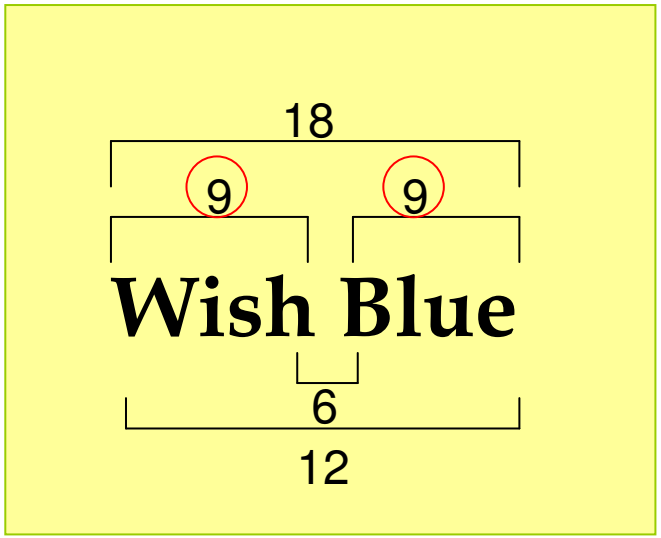
Observations

family	given	1st	2nd	3rd	4th	5th
Ke	Bla	7	7	7	7	14
Wish	Blue	9	9	6	12	18
Hash	Cube	10	9	4	15	19
Ho	Ec	4	4	5	3	8
Gue	Fu	7	4	7	4	11
Stl	Grø	4	7	3	8	11
Si	Ham	2	10	4	8	12
H	J	4	2	4	2	6
Cak	Kec	7	8	6	9	15
Luf	Fa	5	6	6	5	11
Bal	Sha	7	7	2	12	14
Three	SHAvite	16	16	5	27	32
Md	Si	6	2	3	5	8
In	Ske	4	8	4	8	12

Free the SHA-3 rounds parameter

Fact.1

- Almost of "1st number = 2nd number" candidates are alive in second round.
  - Namely, strokes of given name equals that of family name
  - 5 candidates (out of 6)



Blue Midnight Wish

  - Only died candidate is Lux.

Free the SHA-3 rounds parameter

Fact.2

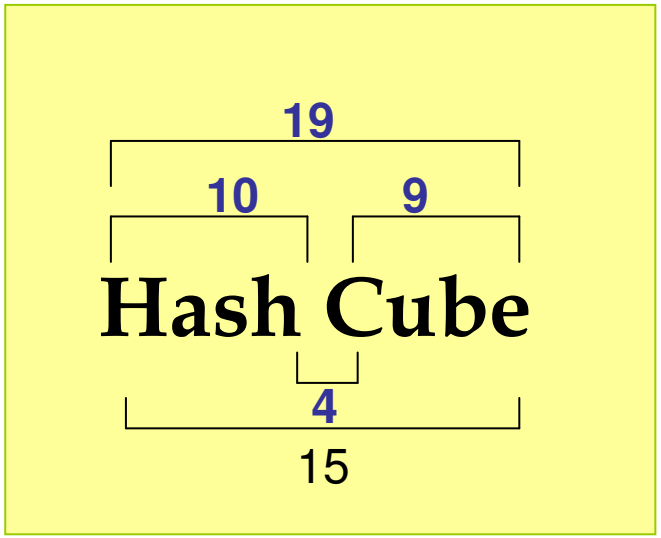
- Scores of alive candidates are terrible.
- In fact,

  "1st number = 2nd number" case is recognized as the worse case…

Free the SHA-3 rounds parameter

Fact.2

- Scores of alive candidates are terrible.
- Another case : CubeHash
  - 4 numbers (of 5) are terrible

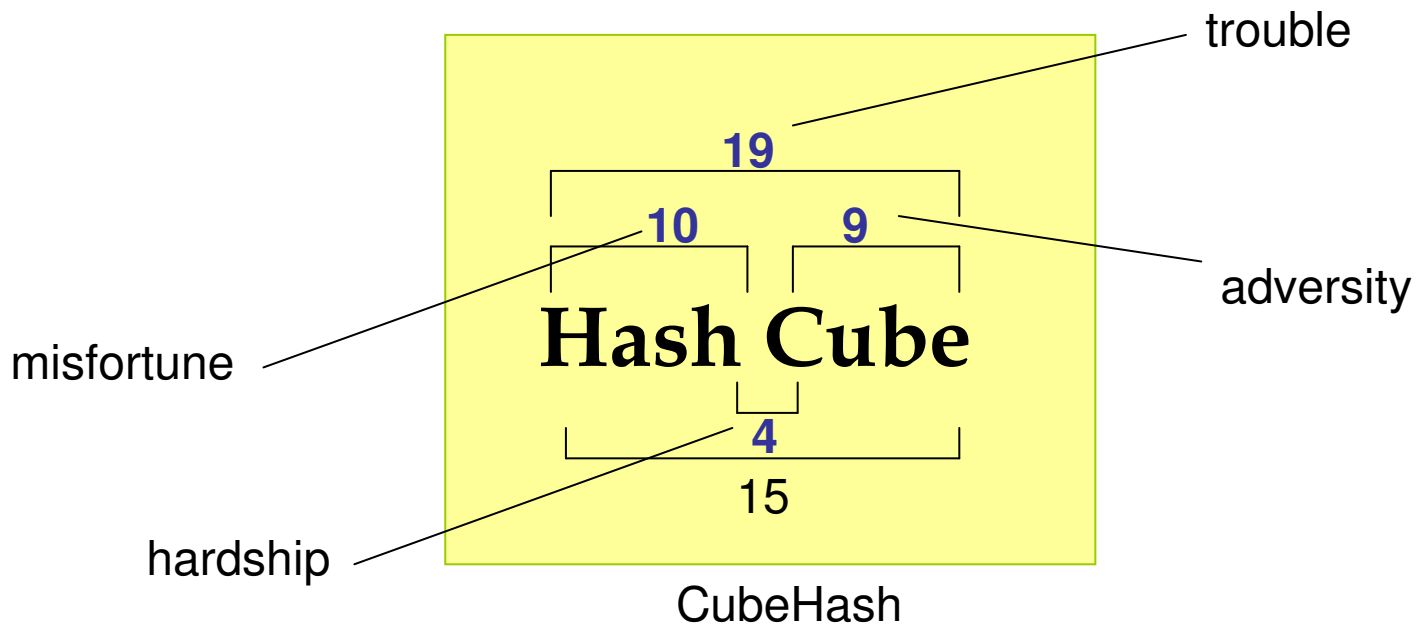


CubeHash

Free the SHA-3 rounds parameter

Fact.2

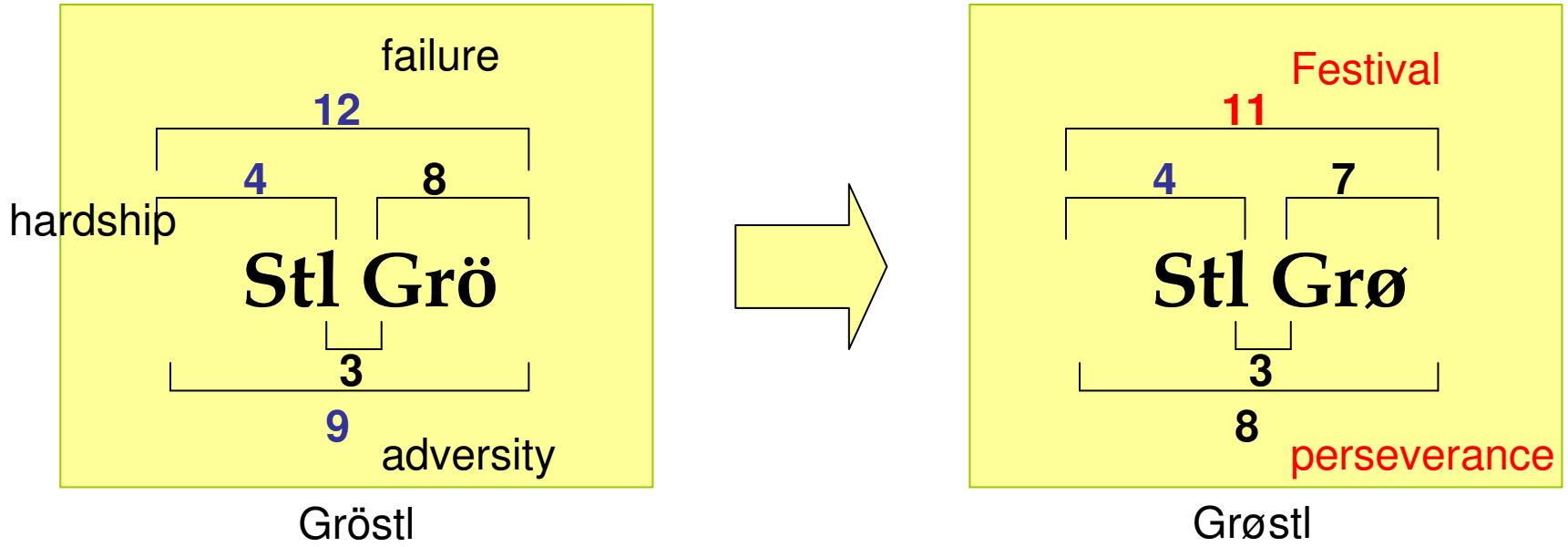
- **Scores of alive candidates are terrible.**
- **Another case : CubeHash**
  - **4 numbers (of 5) are terrible**



Free the SHA-3 rounds parameter

Fact.3

- Don’t worry, Daniel ! I have a good news.
- Only candidate which name were changed



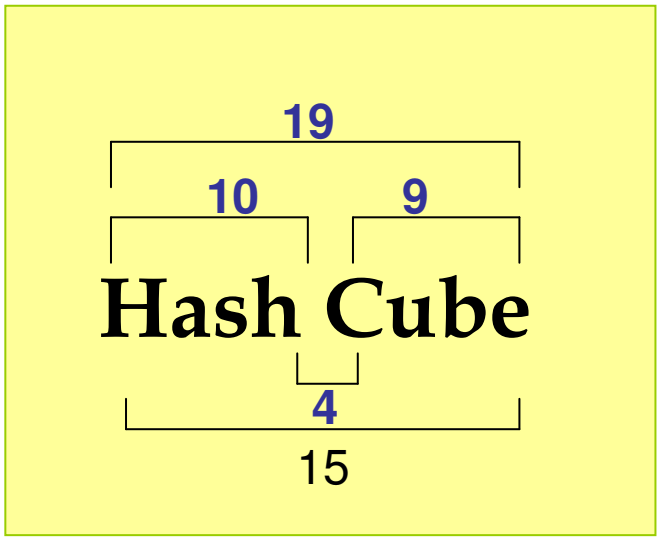
Gröstl

Grøstl

Free the SHA-3 rounds parameter

Fact.4

- I have some new names against CubeHash

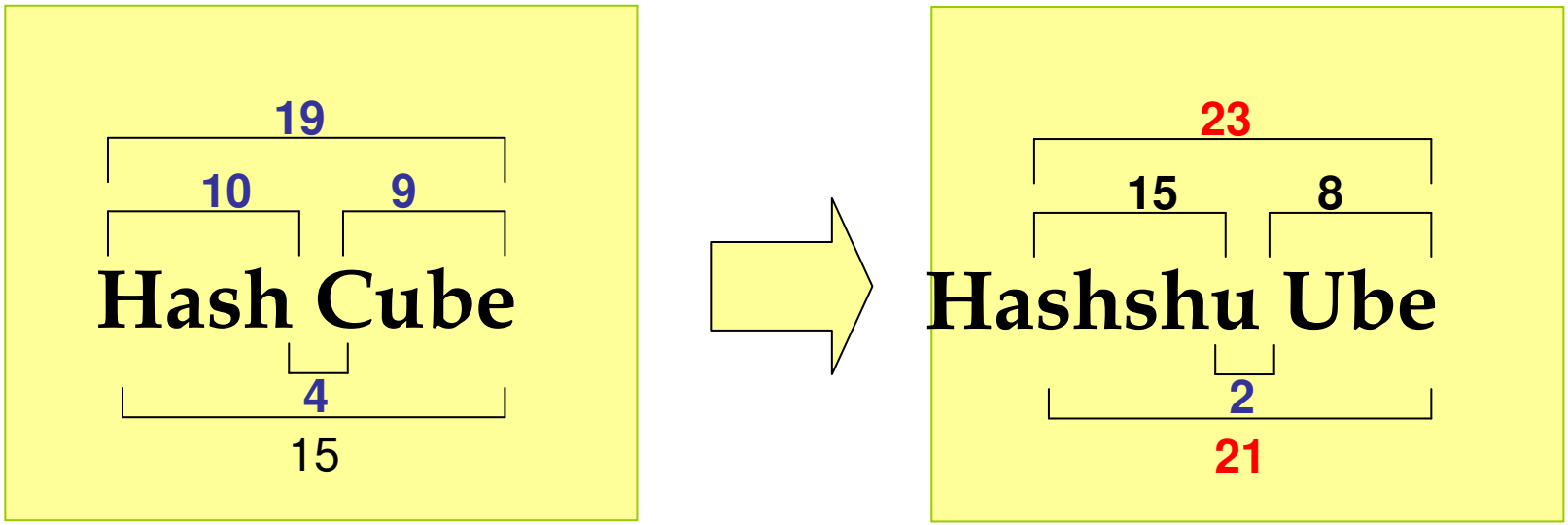


CubeHash

Free the SHA-3 rounds parameter

Fact.4

- I have some new names against CubeHash



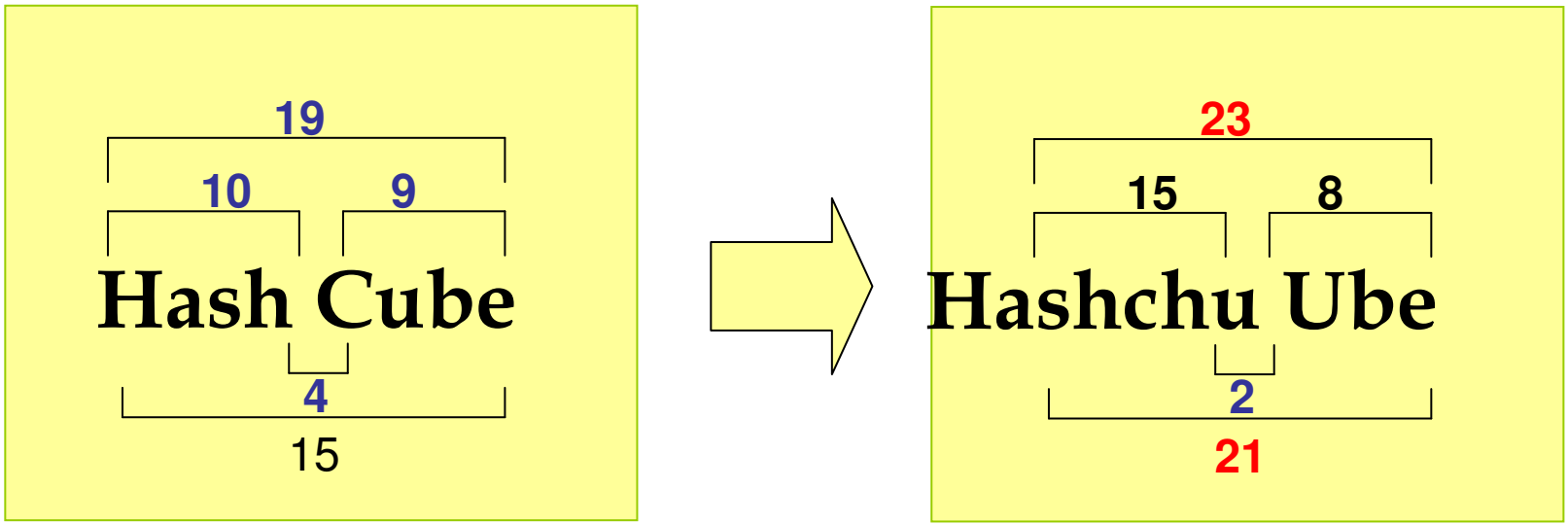
CubeHash

UbeHashshu

Free the SHA-3 rounds parameter

Fact.4

- I have some new names against CubeHash



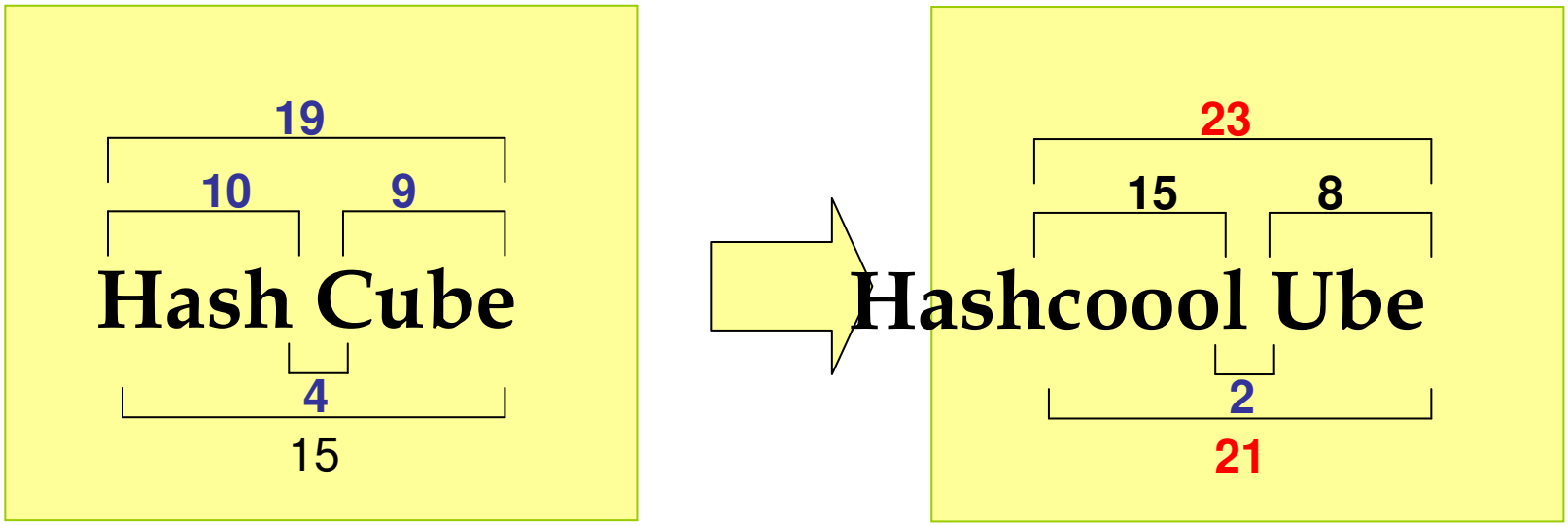
CubeHash

UbeHashchu

Free the SHA-3 rounds parameter

Fact.4

- I have some new names against CubeHash



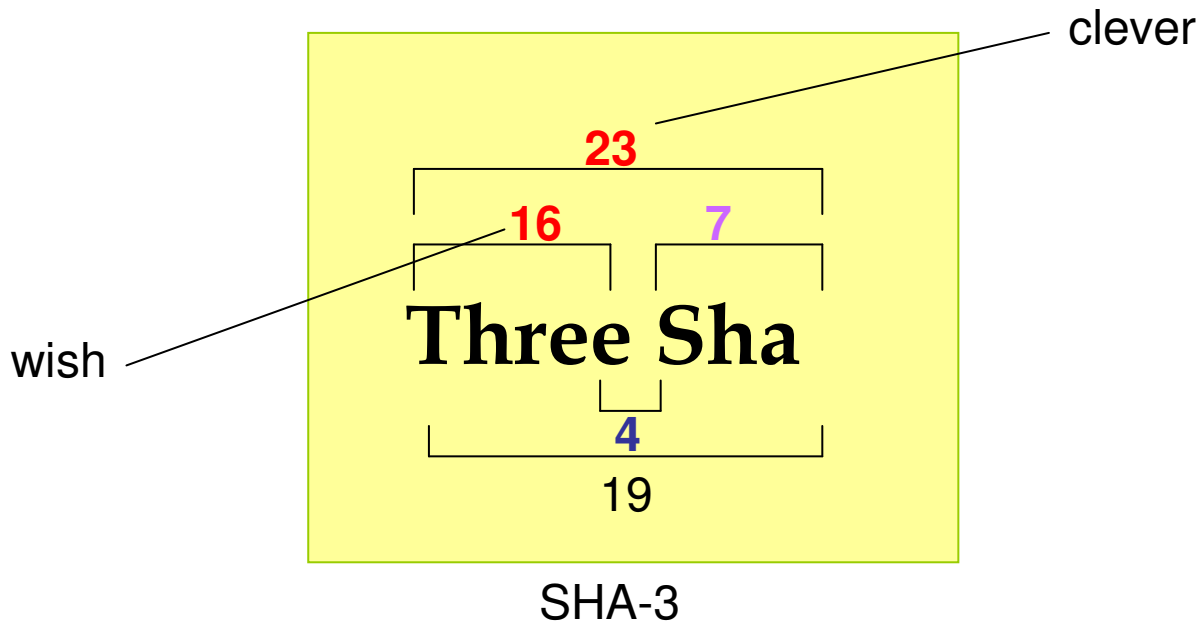
CubeHash

UbeHashcoool

Free the SHA-3 rounds parameter

Fact.5

- **SHA-3 has a good score.**
  - **SHA-4,5 are terrible, SHA-6,7 are so-so.**



Appendix

family	given	1st	2nd	3rd	4th	5th
Us	Abac	2	10	4	8	12
Ari	Rang	7	11	4	14	18
Auro	Ra	8	6	4	10	14
Ke	Bla	7	7	7	7	14
Der	Blen	9	11	6	14	20
Wish	Blue	9	9	6	12	18
Ole	Bo	4	6	7	3	10
Tah	Chee	12	8	4	16	20
Hi	C	4	1	2	3	5
Ch	Crun	4	8	4	8	12
Hash	Cube	10	9	4	15	19

family	given	1st	2nd	3rd	4th	5th
CH	D	4	2	5	1	6
Sha	Dynamic	7	17	5	19	24
Shatwo	Dynamic	14	17	3	28	31
Ho	Ec	4	4	5	3	8
H	Eco	3	5	7	1	8
R	Edon	3	10	7	6	13
Rupt	En	8	7	6	9	15
Ence	ESS	11	6	8	9	17
B	Fs	3	4	6	1	7
Gue	Fu	7	4	7	4	11
Stl	Grø	4	7	3	8	11
Stl	Grö	4	8	3	9	12
Si	Ham	2	10	4	8	12
H	J	4	2	4	2	6
Cak	Kec	7	8	6	9	15

family	given	1st	2nd	3rd	4th	5th
One	Khichidi	8	15	7	16	23
Ne	La	7	4	5	6	11
Lesa	Mnta	9	12	7	14	21
Luf	Fa	5	6	6	5	11
X	Lu	2	2	3	1	4
Three	Mcssha	16	13	8	21	29
Six	Md	4	6	6	4	10
Five	Md	10	6	8	8	16
Seven	Md	14	6	7	13	20
Eight	Md	13	6	6	13	19
Nine	Md	11	6	8	9	17
Hash	Mesh	10	12	7	15	22
Sha	Na	7	6	6	7	13
Strorm	Sand	14	9	5	18	23
Mal	Sar	8	7	2	13	15

family	given	1st	2nd	3rd	4th	5th
Ail	Sg	5	3	2	6	8
Bal	Sha	7	7	2	12	14
Mata	Sha	12	7	4	15	19
Three	SHAvite	16	16	5	27	32
Md	Si	6	2	3	5	8
In	Ske	4	8	4	8	12
Hash	Spectral	10	17	4	23	27
Hash	Stream	10	17	4	23	27
Tx	Swiff	4	12	3	13	16
Angle	T	13	2	6	9	15
Three	Tib	16	6	6	16	22
Er	Twist	7	10	5	12	17
Tex	Vor	8	6	4	10	14
Mm	Wa	8	7	8	7	15
Fall	Water	8	16	5	19	24

family	given	1st	2nd	3rd	4th	5th
Three	Sha	16	7	5	18	23
Two	Sha	7	7	2	12	14
One	Sha	8	7	5	10	15
Four	Sha	8	7	4	11	15
Five	Sha	10	7	5	12	17
Six	Sha	4	7	3	8	11
Seven	Sha	14	7	4	17	21