Starting point

Starting point

- Classical construction by Majewski, Wormald, Havas and Czech (MWHC), 1996

Starting point

- Classical construction by Majewski, Wormald, Havas and Czech (MWHC), 1996
- Pick 2 random hash function h, g: $|U| \rightarrow cn$, with $c > 1$

Starting point

- Classical construction by Majewski, Wormald, Havas and Czech (MWHC), 1996
- Pick 2 random hash function h, g: $|U| \rightarrow cn$, with $c > 1$
- Solve the random $\mathbf{F}_2$-linear system $v_{g(x)} \oplus v_{h(x)} = f(x)$

Starting point

- Classical construction by Majewski, Wormald, Havas and Czech (MWHC), 1996
- Pick 2 random hash function h, g: $|U| \rightarrow cn$, with $c > 1$
- Solve the random $\mathbf{F}_2$-linear system $v_{g(x)} \oplus v_{h(x)} = f(x)$
- If $c > 2.09$ the random graph with edges $g(x)$—$h(x)$ is almost surely *acyclic* as $n \rightarrow \infty$

Starting point

- Classical construction by Majewski, Wormald, Havas and Czech (MWHC), 1996
- Pick 2 random hash function h, g: $|U| \to cn$, with $c > 1$
- Solve the random $\mathbf{F}_2$-linear system $v_{g(x)} \oplus v_{h(x)} = f(x)$
- If $c > 2.09$ the random graph with edges $g(x)$—$h(x)$ is almost surely *acyclic* as $n \to \infty$
- We *peel* the graph removing leaves iteratively

Starting point

- Classical construction by Majewski, Wormald, Havas and Czech (MWHC), 1996
- Pick 2 random hash function h, g: $|U| \to cn$, with $c > 1$
- Solve the random $\mathbf{F}_2$-linear system $v_{g(x)} \oplus v_{h(x)} = f(x)$
- If $c > 2.09$ the random graph with edges $g(x)$—$h(x)$ is almost surely *acyclic* as $n \to \infty$
- We *peel* the graph removing leaves iteratively
- Every edge is associated with the leaf that caused its removal

An example

An example

$f:X \to [16]$

$z \mapsto 0$

$a \mapsto 3$

$p \mapsto 11$

$u \mapsto 7$

$c \mapsto 2$

An example

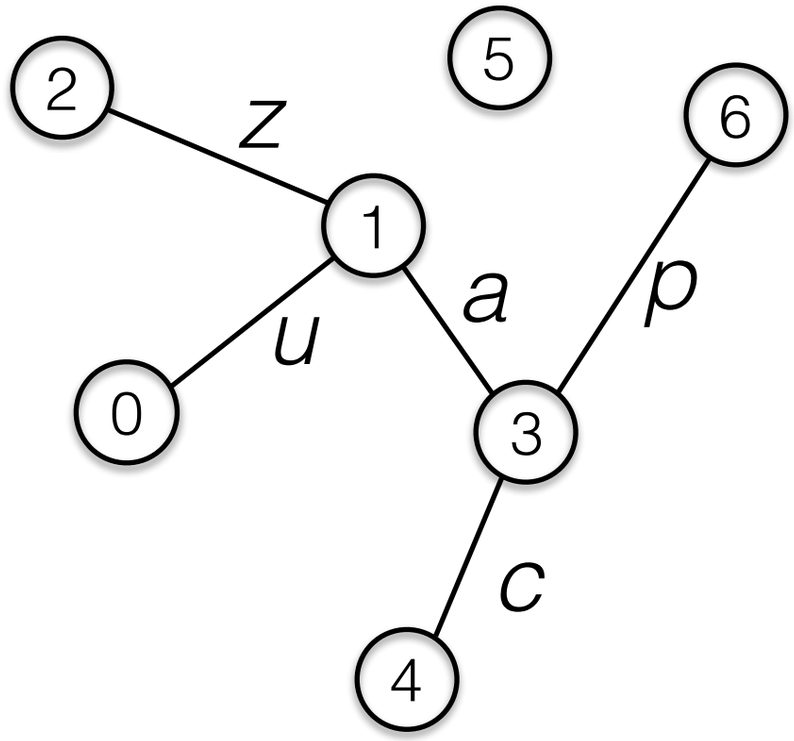
$f:X \to [16]$	$g:U \to [7]$
$z \mapsto 0$	$z \mapsto 1$
$a \mapsto 3$	$a \mapsto 3$
$p \mapsto 11$	$p \mapsto 3$
$u \mapsto 7$	$u \mapsto 1$
$c \mapsto 2$	$c \mapsto 4$

An example

$f:X \to [16]$	$g:U \to [7]$	$h:U \to [7]$
$z \mapsto 0$	$z \mapsto 1$	$z \mapsto 2$
$a \mapsto 3$	$a \mapsto 3$	$a \mapsto 1$
$p \mapsto 11$	$p \mapsto 3$	$p \mapsto 6$
$u \mapsto 7$	$u \mapsto 1$	$u \mapsto 0$
$c \mapsto 2$	$c \mapsto 4$	$c \mapsto 3$

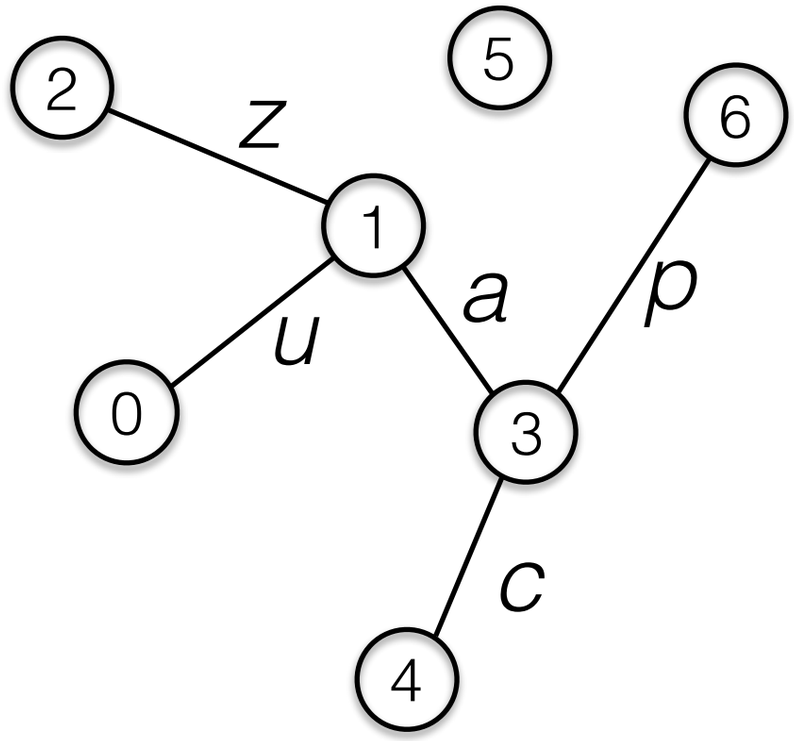
An example

$f:X \to [16]$	$g:U \to [7]$	$h:U \to [7]$
$z \mapsto 0$	$z \mapsto 1$	$z \mapsto 2$
$a \mapsto 3$	$a \mapsto 3$	$a \mapsto 1$
$p \mapsto 11$	$p \mapsto 3$	$p \mapsto 6$
$u \mapsto 7$	$u \mapsto 1$	$u \mapsto 0$
$c \mapsto 2$	$c \mapsto 4$	$c \mapsto 3$



An example

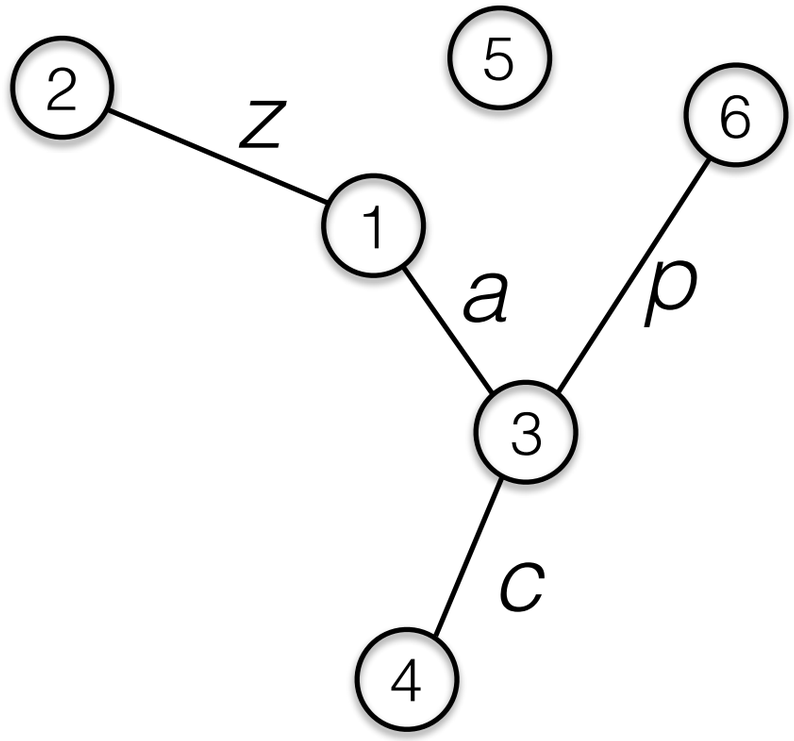
$f:X \to [16]$	$g:U \to [7]$	$h:U \to [7]$
$z \mapsto 0$	$z \mapsto 1$	$z \mapsto 2$
$a \mapsto 3$	$a \mapsto 3$	$a \mapsto 1$
$p \mapsto 11$	$p \mapsto 3$	$p \mapsto 6$
$u \mapsto 7$	$u \mapsto 1$	$u \mapsto 0$
$c \mapsto 2$	$c \mapsto 4$	$c \mapsto 3$



$$v_1 \oplus \boldsymbol{v_0} = f(u) = 7$$

An example

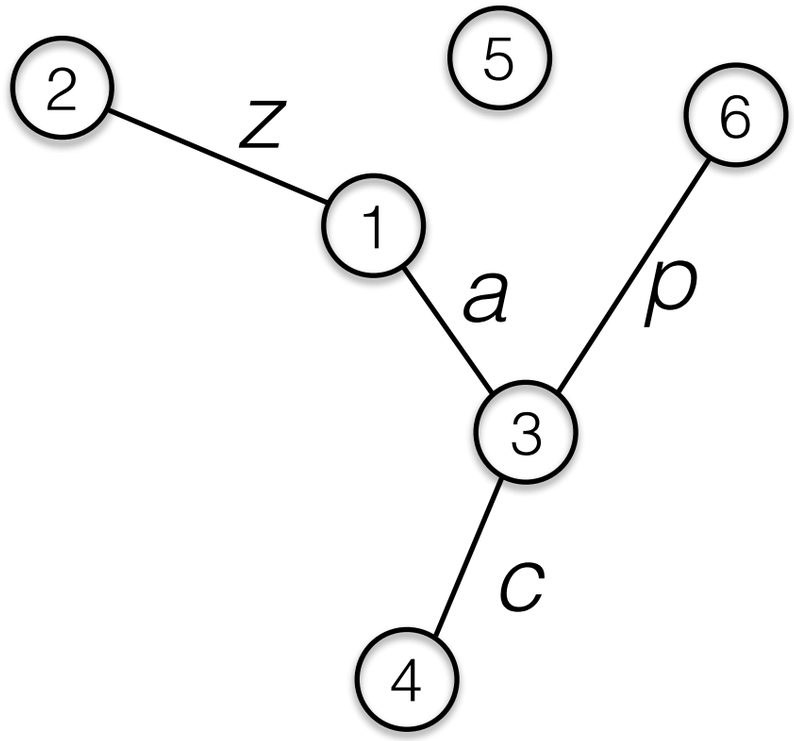
$f:X \to [16]$	$g:U \to [7]$	$h:U \to [7]$
$z \mapsto 0$	$z \mapsto 1$	$z \mapsto 2$
$a \mapsto 3$	$a \mapsto 3$	$a \mapsto 1$
$p \mapsto 11$	$p \mapsto 3$	$p \mapsto 6$
$u \mapsto 7$	$u \mapsto 1$	$u \mapsto 0$
$c \mapsto 2$	$c \mapsto 4$	$c \mapsto 3$



$$v_1 \oplus \boldsymbol{v_0} = f(u) = 7$$

An example

$f:X \to [16]$	$g:U \to [7]$	$h:U \to [7]$
$z \mapsto 0$	$z \mapsto 1$	$z \mapsto 2$
$a \mapsto 3$	$a \mapsto 3$	$a \mapsto 1$
$p \mapsto 11$	$p \mapsto 3$	$p \mapsto 6$
$u \mapsto 7$	$u \mapsto 1$	$u \mapsto 0$
$c \mapsto 2$	$c \mapsto 4$	$c \mapsto 3$

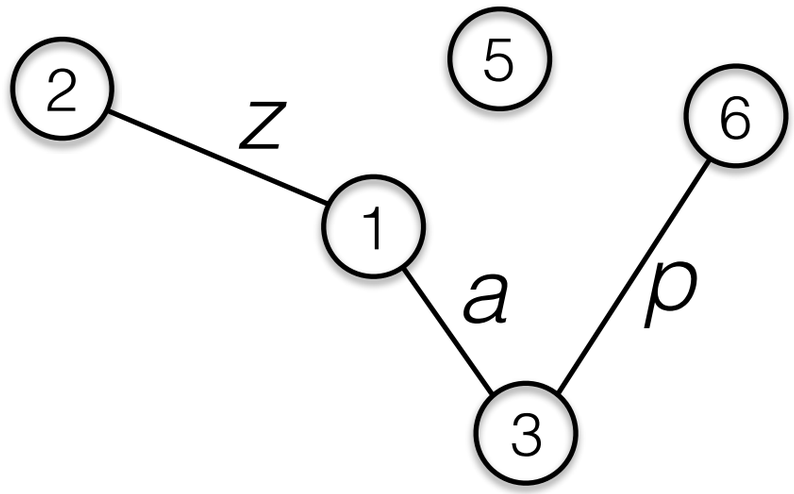


$$\boldsymbol{v_4} \oplus v_3 = f(c) = 2$$

$$v_1 \oplus \boldsymbol{v_0} = f(u) = 7$$

An example

$f:X \to [16]$	$g:U \to [7]$	$h:U \to [7]$
$z \mapsto 0$	$z \mapsto 1$	$z \mapsto 2$
$a \mapsto 3$	$a \mapsto 3$	$a \mapsto 1$
$p \mapsto 11$	$p \mapsto 3$	$p \mapsto 6$
$u \mapsto 7$	$u \mapsto 1$	$u \mapsto 0$
$c \mapsto 2$	$c \mapsto 4$	$c \mapsto 3$

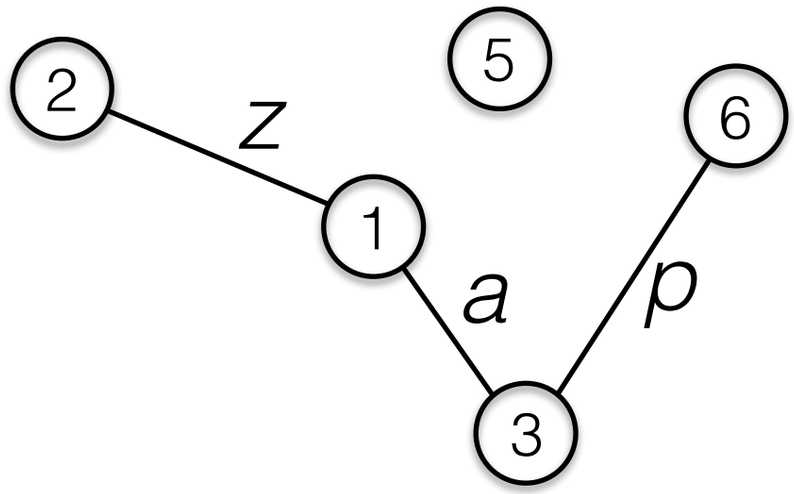


$$\boldsymbol{v_4} \oplus v_3 = f(c) = 2$$

$$v_1 \oplus \boldsymbol{v_0} = f(u) = 7$$

An example

$f:X \to [16]$	$g:U \to [7]$	$h:U \to [7]$
$z \mapsto 0$	$z \mapsto 1$	$z \mapsto 2$
$a \mapsto 3$	$a \mapsto 3$	$a \mapsto 1$
$p \mapsto 11$	$p \mapsto 3$	$p \mapsto 6$
$u \mapsto 7$	$u \mapsto 1$	$u \mapsto 0$
$c \mapsto 2$	$c \mapsto 4$	$c \mapsto 3$



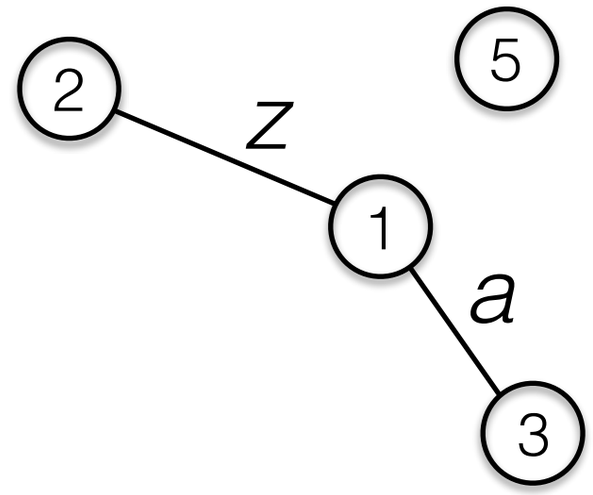
$$v_3 \oplus \boldsymbol{v_6} = f(p) = 11$$

$$\boldsymbol{v_4} \oplus v_3 = f(c) = 2$$

$$v_1 \oplus \boldsymbol{v_0} = f(u) = 7$$

An example

$f:X \to [16]$	$g:U \to [7]$	$h:U \to [7]$
$z \mapsto 0$	$z \mapsto 1$	$z \mapsto 2$
$a \mapsto 3$	$a \mapsto 3$	$a \mapsto 1$
$p \mapsto 11$	$p \mapsto 3$	$p \mapsto 6$
$u \mapsto 7$	$u \mapsto 1$	$u \mapsto 0$
$c \mapsto 2$	$c \mapsto 4$	$c \mapsto 3$



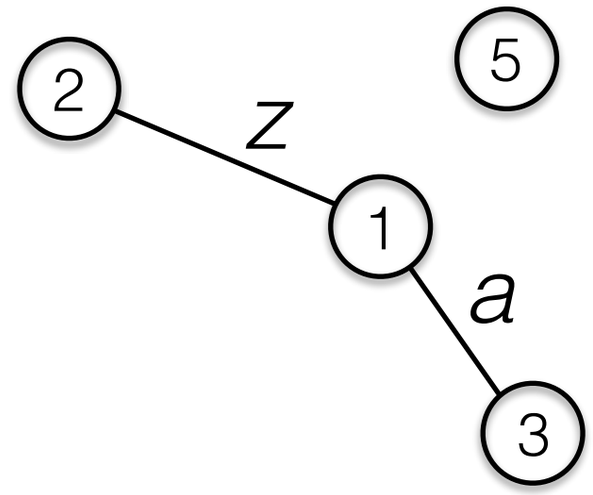
$$v_3 \oplus \boldsymbol{v_6} = f(p) = 11$$

$$\boldsymbol{v_4} \oplus v_3 = f(c) = 2$$

$$v_1 \oplus \boldsymbol{v_0} = f(u) = 7$$

An example

$f:X \to [16]$	$g:U \to [7]$	$h:U \to [7]$
$z \mapsto 0$	$z \mapsto 1$	$z \mapsto 2$
$a \mapsto 3$	$a \mapsto 3$	$a \mapsto 1$
$p \mapsto 11$	$p \mapsto 3$	$p \mapsto 6$
$u \mapsto 7$	$u \mapsto 1$	$u \mapsto 0$
$c \mapsto 2$	$c \mapsto 4$	$c \mapsto 3$



$$v_1 \oplus \boldsymbol{v_2} = f(z) = 0$$

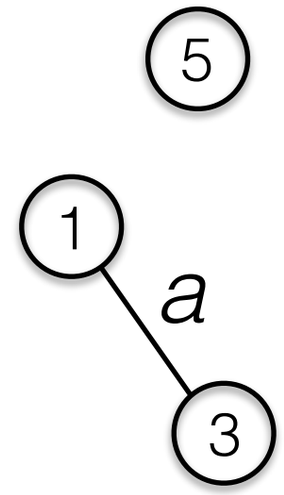
$$v_3 \oplus \boldsymbol{v_6} = f(p) = 11$$

$$\boldsymbol{v_4} \oplus v_3 = f(c) = 2$$

$$v_1 \oplus \boldsymbol{v_0} = f(u) = 7$$

An example

$f:X \to [16]$	$g:U \to [7]$	$h:U \to [7]$
$z \mapsto 0$	$z \mapsto 1$	$z \mapsto 2$
$a \mapsto 3$	$a \mapsto 3$	$a \mapsto 1$
$p \mapsto 11$	$p \mapsto 3$	$p \mapsto 6$
$u \mapsto 7$	$u \mapsto 1$	$u \mapsto 0$
$c \mapsto 2$	$c \mapsto 4$	$c \mapsto 3$



$$v_1 \oplus \boldsymbol{v_2} = f(z) = 0$$

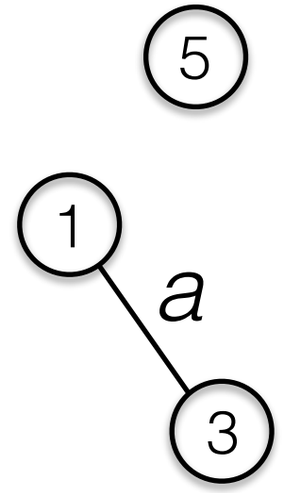
$$v_3 \oplus \boldsymbol{v_6} = f(p) = 11$$

$$\boldsymbol{v_4} \oplus v_3 = f(c) = 2$$

$$v_1 \oplus \boldsymbol{v_0} = f(u) = 7$$

An example

$f:X \to [16]$	$g:U \to [7]$	$h:U \to [7]$
$z \mapsto 0$	$z \mapsto 1$	$z \mapsto 2$
$a \mapsto 3$	$a \mapsto 3$	$a \mapsto 1$
$p \mapsto 11$	$p \mapsto 3$	$p \mapsto 6$
$u \mapsto 7$	$u \mapsto 1$	$u \mapsto 0$
$c \mapsto 2$	$c \mapsto 4$	$c \mapsto 3$



$$v_3 \oplus \boldsymbol{v_1} = f(a) = 3$$

$$v_1 \oplus \boldsymbol{v_2} = f(z) = 0$$

$$v_3 \oplus \boldsymbol{v_6} = f(p) = 11$$

$$\boldsymbol{v_4} \oplus v_3 = f(c) = 2$$

$$v_1 \oplus \boldsymbol{v_0} = f(u) = 7$$

An example

$f:X \to [16]$	$g:U \to [7]$	$h:U \to [7]$
$z \mapsto 0$	$z \mapsto 1$	$z \mapsto 2$
$a \mapsto 3$	$a \mapsto 3$	$a \mapsto 1$
$p \mapsto 11$	$p \mapsto 3$	$p \mapsto 6$
$u \mapsto 7$	$u \mapsto 1$	$u \mapsto 0$
$c \mapsto 2$	$c \mapsto 4$	$c \mapsto 3$

5

3

$v_3 \oplus \boldsymbol{v_1} = f(a) = 3$

$v_1 \oplus \boldsymbol{v_2} = f(z) = 0$

$v_3 \oplus \boldsymbol{v_6} = f(p) = 11$

$\boldsymbol{v_4} \oplus v_3 = f(c) = 2$

$v_1 \oplus \boldsymbol{v_0} = f(u) = 7$

An example

$f:X \to [16]$	$g:U \to [7]$	$h:U \to [7]$
$z \mapsto 0$	$z \mapsto 1$	$z \mapsto 2$
$a \mapsto 3$	$a \mapsto 3$	$a \mapsto 1$
$p \mapsto 11$	$p \mapsto 3$	$p \mapsto 6$
$u \mapsto 7$	$u \mapsto 1$	$u \mapsto 0$
$c \mapsto 2$	$c \mapsto 4$	$c \mapsto 3$

5

3

$v_3 \oplus \boldsymbol{v_1} = f(a) = 3$

$v_1 \oplus \boldsymbol{v_2} = f(z) = 0$

$v_3 \oplus \boldsymbol{v_6} = f(p) = 11$

$\boldsymbol{v_4} \oplus v_3 = f(c) = 2$

$v_1 \oplus \boldsymbol{v_0} = f(u) = 7$

$v_3 = 0,\ \boldsymbol{v_1} = 3$

An example

$f:X \to [16]$	$g:U \to [7]$	$h:U \to [7]$
$z \mapsto 0$	$z \mapsto 1$	$z \mapsto 2$
$a \mapsto 3$	$a \mapsto 3$	$a \mapsto 1$
$p \mapsto 11$	$p \mapsto 3$	$p \mapsto 6$
$u \mapsto 7$	$u \mapsto 1$	$u \mapsto 0$
$c \mapsto 2$	$c \mapsto 4$	$c \mapsto 3$

(5)

(3)

$v_3 \oplus \boldsymbol{v_1} = f(a) = 3$

$v_1 \oplus \boldsymbol{v_2} = f(z) = 0$

$v_3 \oplus \boldsymbol{v_6} = f(p) = 11$

$\boldsymbol{v_4} \oplus v_3 = f(c) = 2$

$v_1 \oplus \boldsymbol{v_0} = f(u) = 7$

$v_3 = 0,\ \boldsymbol{v_1} = 3$

$\boldsymbol{v_2} = v_1 \oplus 0 = 3$

An example

$f:X \to [16]$	$g:U \to [7]$	$h:U \to [7]$
$z \mapsto 0$	$z \mapsto 1$	$z \mapsto 2$
$a \mapsto 3$	$a \mapsto 3$	$a \mapsto 1$
$p \mapsto 11$	$p \mapsto 3$	$p \mapsto 6$
$u \mapsto 7$	$u \mapsto 1$	$u \mapsto 0$
$c \mapsto 2$	$c \mapsto 4$	$c \mapsto 3$

(5)

(3)

$v_3 \oplus \boldsymbol{v_1} = f(a) = 3$ $\quad v_3 = 0,\ \boldsymbol{v_1} = 3$

$v_1 \oplus \boldsymbol{v_2} = f(z) = 0$ $\quad \boldsymbol{v_2} = v_1 \oplus 0 = 3$

$v_3 \oplus \boldsymbol{v_6} = f(p) = 11$ $\quad \boldsymbol{v_6} = v_3 \oplus 11 = 11$

$\boldsymbol{v_4} \oplus v_3 = f(c) = 2$

$v_1 \oplus \boldsymbol{v_0} = f(u) = 7$

An example

$f:X \to [16]$	$g:U \to [7]$	$h:U \to [7]$
$z \mapsto 0$	$z \mapsto 1$	$z \mapsto 2$
$a \mapsto 3$	$a \mapsto 3$	$a \mapsto 1$
$p \mapsto 11$	$p \mapsto 3$	$p \mapsto 6$
$u \mapsto 7$	$u \mapsto 1$	$u \mapsto 0$
$c \mapsto 2$	$c \mapsto 4$	$c \mapsto 3$

(5)

(3)

$v_3 \oplus \boldsymbol{v_1} = f(a) = 3$ $\quad v_3 = 0,\ \boldsymbol{v_1} = 3$

$v_1 \oplus \boldsymbol{v_2} = f(z) = 0$ $\quad \boldsymbol{v_2} = v_1 \oplus 0 = 3$

$v_3 \oplus \boldsymbol{v_6} = f(p) = 11$ $\quad \boldsymbol{v_6} = v_3 \oplus 11 = 11$

$\boldsymbol{v_4} \oplus v_3 = f(c) = 2$ $\quad \boldsymbol{v_4} = v_3 \oplus 2 = 2$

$v_1 \oplus \boldsymbol{v_0} = f(u) = 7$

An example

$f:X \to [16]$	$g:U \to [7]$	$h:U \to [7]$
$z \mapsto 0$	$z \mapsto 1$	$z \mapsto 2$
$a \mapsto 3$	$a \mapsto 3$	$a \mapsto 1$
$p \mapsto 11$	$p \mapsto 3$	$p \mapsto 6$
$u \mapsto 7$	$u \mapsto 1$	$u \mapsto 0$
$c \mapsto 2$	$c \mapsto 4$	$c \mapsto 3$

5

3

$v_3 \oplus \boldsymbol{v_1} = f(a) = 3$	$v_3 = 0,\ \boldsymbol{v_1} = 3$
$v_1 \oplus \boldsymbol{v_2} = f(z) = 0$	$\boldsymbol{v_2} = v_1 \oplus 0 = 3$
$v_3 \oplus \boldsymbol{v_6} = f(p) = 11$	$\boldsymbol{v_6} = v_3 \oplus 11 = 11$
$\boldsymbol{v_4} \oplus v_3 = f(c) = 2$	$\boldsymbol{v_4} = v_3 \oplus 2 = 2$
$v_1 \oplus \boldsymbol{v_0} = f(u) = 7$	$\boldsymbol{v_0} = v_1 \oplus 7 = 4$