環

学習指導要領（3）- 知・技 - ア
学習指導要領（3）- 知・技 - イ
学習指導要領（3）- 思・判・表 - イ
学習内容（3）- ア コンピュータの仕組みと処理
学習内容（3）- イ アルゴリズムとプログラム

情報III

(ア) $y = h(x)$ を、任意のビット列 x を引数にとり、16 ビットの値 (ハッシュ値)y を返すハッシュ関数とする。ただし、y を与えて x を求める方法は知られていない。

(a) 任意のビット列 a と 20 ビットの値 b から成るデータにおいて、a はそのままに b だけを変化させて、ハッシュ値 $y_1 = h(concat(a, b))$ を任意の値にすることを考える。ここで、関数 $concat$ は 2 つのビット列を連結する関数であり、 例えば $concat(001111, 00)$ は 00111100 となる。

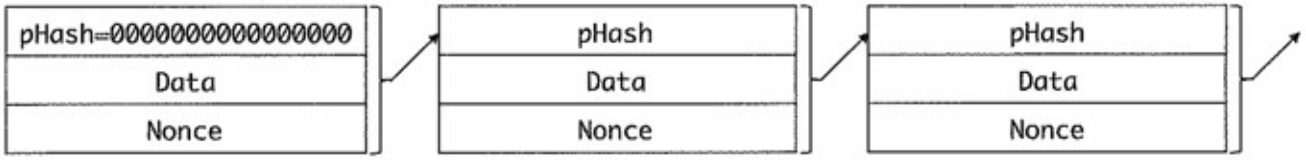
ハッシュ関数の特性から、y_1 からハッシュ関数に渡す引数 $concat(a, b)$ を計算することはできず、そのため b も計算することはできない。よってハッシュ値が y_1 となるような b を選ぶためには、任意の b を選んでハッシュ値を計算する作業を、計算したハッシュ値が y_1 になるまで繰り返す必要がある。ハッシュ関数 $y = h(x)$ は、x から y を計算したときに y の出現確率が同じでなければならないとすると、この方法でハッシュ値が y_1 になるように b を選ぶのに必要なハッシュ値の計算回数の期待値は (19)(20)(21)(22)(23)(24)(25) 回である。これは、次のようにして求めることができる。

$$\frac{1}{2} \cdot 2^{(26)(27)}$$

また、ハッシュ値 y_2 の上位 8 ビットが 0 になるような b を選ぶのに必要なハッシュ値の計算回数の期待値は (28)(29)(30)(31)(32)(33)(34) 回である。ただし、y_2 の下位 8 ビットは何でもよいものとする。これは、次のようにして求めることができる。

$$\frac{1}{2} \cdot 2^{(35)(36)}$$

(イ) 16 ビットの値 pHash、任意のビット列 Data、32 ビットの値 Nonce から成るデータセットを考え、pHash, Data, Nonce を連結したビット列をブロックと呼ぶこととする。ここで、ハッシュ関数 h を用いて下図のように pHash に前のブロックのハッシュ値を入れることによってブロックのチェーンを作ることを考える。ただし、チェーンの 1 つ目のブロックの pHash は 0 が 16 個並んだものとする。また、それぞれのブロックのハッシュ値の上位 8 ビットは 0 でなければならないものとする。ただし、ハッシュ値の下位 8 ビットは何でもよいものとする。



(a) 1 つ目のブロックが外部から与えられたとする。2 つ目のブロックの Data が決まっている状態で、2 つ目のブロックを生成するために 2 つ目のブロックの Nonce を選ぶのに必要なハッシュ値の計算回数

の期待値は (37)(38)(39)(40)(41)(42)(43) 回である。これは、次のようにして求めることができる。

$$\frac{1}{2} \cdot 2^{(44)(45)} + (46)(47)$$

(b) 10 個のブロックが外部から与えられたとき、3 つ目のブロックの Data を変更することを考える。10 個のブロック全ての辻褄が合うようにするために必要なハッシュ値の計算回数の期待値は (48)(49)(50)(51)(52)(53)(54)(55) 回である。これは、次のようにして求めることができる。

$$\frac{1}{2} \cdot 2^{(44)(45)} \cdot (56)(57) + (58)(59)$$