Subject: جلسه ۱۷
Year. ۱۴۰۰ Month. ۹ Date. ۲ ( )

روش سوم: هش دوگانه یا Double Hashing

۲ تابع هش داریم: h_1 و h_2

$h_1(x) - h_1(x) + h_2(x) - h_1(x) + 2h_2(x) - \dots$

$h_1(x) = x \% 12$ — $h_2(x) = 2x \% 5$

$x = 24$ ۰-۲-۴-۶-۸-...

* $h_2(x)$ هیچ‌گاه صفر نشود
* همه جدول یا بیش‌تا حل‌ها در جدول را دور بزند.
* N ← عدد اول
* $N > n$ ← ضریب ۲، ۳... بیشتر باشد این خواهیم نیل بزرگ‌تر از n باشد و در عین حال تا به برابر باشند (اختلاف کمی داشته باشند)

تعادم غ‌غ: $|u| \gg N$

مشکل تمام روش‌های درهم‌سازی این است که اگر کسی بتواند از تابع Hash اطلاع داشته باشد می‌تواند ورودی بد بدهد. (Adversary)

راه‌حل این مشکل: استفاده از رندم.

ایده‌ی اصلی: تعدادی تابع درهم‌سازی داشته باشیم و در هنگام اجرا یکی از آن‌ها را به صورت تصادفی انتخاب کنیم.

تعریف: فرض کنید H یک مجموعه از توابع درهم سازی با شد در این صورت H یک مجموعه‌ی جهانی یا universal (خانواده) است اگر

$$\forall x,y \in U \quad , \quad \Pr_{h \in H}[h(x)=h(y)] \leq \frac{1}{N}$$

در واقع تعداد توابعی از H که در آن $h(x)=h(y)$ کمتر از $\frac{|H|}{N}$ است

$$\frac{1}{|H|} \times \frac{|H|}{N} = \frac{1}{N}$$

قضیه: فرض کنید H یک خانواده جهانی است و h یک تابع تصادفی از H است. در این صورت به ازای n دلخواه، متوسط تعداد تصادم‌ها $\frac{n}{N}$ برای یک کلید است.

اثبات: کلید x را در نظر بگیرید به ازای هر کلید $y \neq x$ احتمال تصادم $\frac{1}{N}$ است.
لذا متوسط تصادم‌ها $\frac{n}{N}$ برای یک کلید است.

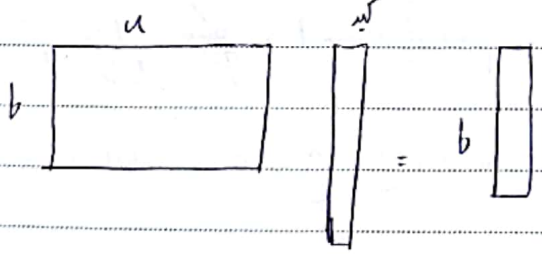
مثال:

فرض کنید U شامل تمام اعداد دویی است. فرض کنید N برابر با توان ۲ است. $b \ll u$

$u = 7 \qquad |U| = 2^u = 2^7 = 128$

$b = 3 \qquad N = 8$

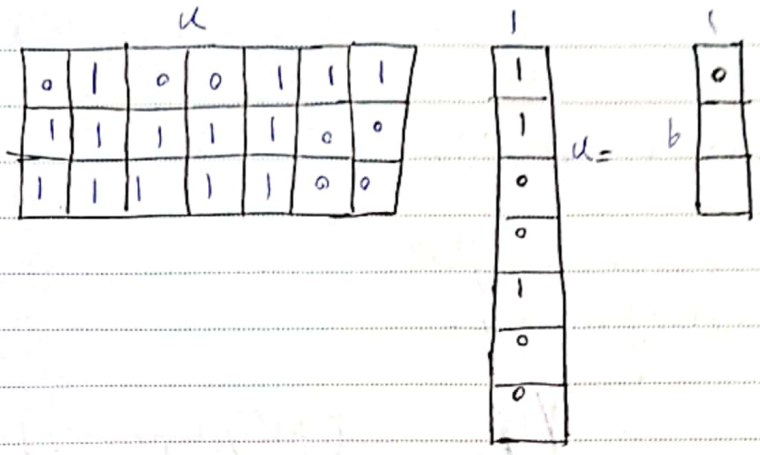
مجموعه H: تمام ماتریس‌های با اندازه $u \times b$ با مقدارهای ۰ و ۱



Subject: ۱۷ جلسه
Year. ۱۴۰۰ Month. ۹ Date. ۲ ( )

$|H| = 2^{bd}$ یکی از توابع H به صورت تصادفی انتخاب می‌شود.

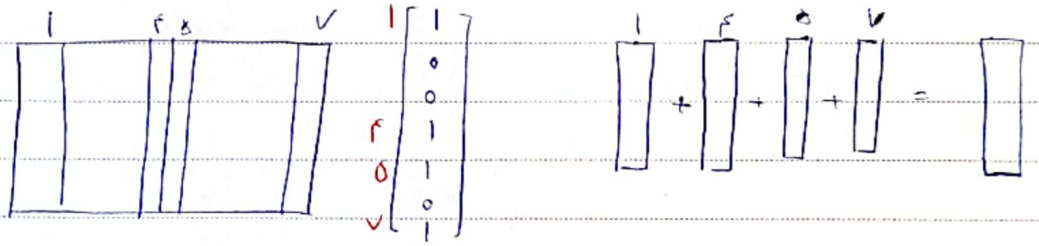
$|u| = 7$
$|b| = 2$



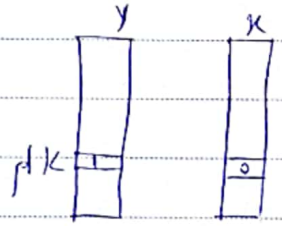
قضیه: فرض کنید h به صورت تصادفی از H انتخاب شده در این صورت:

$\forall x \neq y \quad Pr[h(x) = h(y)] = \frac{1}{2^b} = \frac{1}{2}$

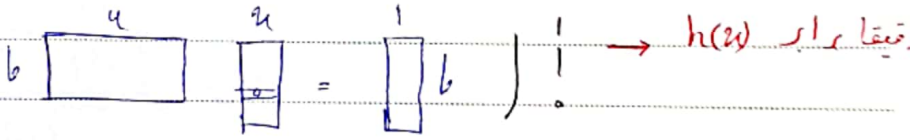
اثبات:

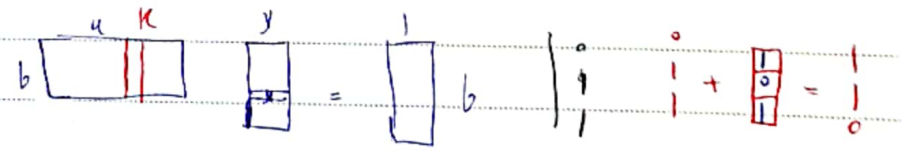


* مثال ۲ کنید $x \neq y$ را در نظر بگیرید: چون $x \neq y$ حداقل یک سطر در x و y متفاوت است.



این سطر را کنار هم گذاریم دستدار Hash را بدون در نظر گرفتن این سطر محاسبه کنید.





Subject: IV ads
Year. ۱۴۰۰ Month. ۹ Date. ۲ ( )

ستون k در h باید چه باشد که $h(x) = h(y)$ باشد؟

۱
۰
۱

احتمال اینکه ستون k چگونه‌ای باشد که $h(x) = h(y)$ باشد $= \frac{1}{2^b}$

مثال: $h_{ab}(x) = ((ax+b) \% p) \% N$

p عدد اول و $> b$

$H = h_{ab} \mid 0 \le a, b \le p-1, a \neq 0$

تعریف تابع هش کامل (تابع درهم‌سازی کامل):

مجموعه‌ی داده‌ی کلیدها داده شده است. تابع هش که بدون تصادم این کلیدها را در A ذخیره کند یک تابع هش کامل است.

تصادم $(1)O$