КРИПТОГРАФСКЕ ХЕШ ФУНКЦИЈЕ: МАТЕМАТИЧКИ УВОД

Коста Чоловић

17. јануар 2026.

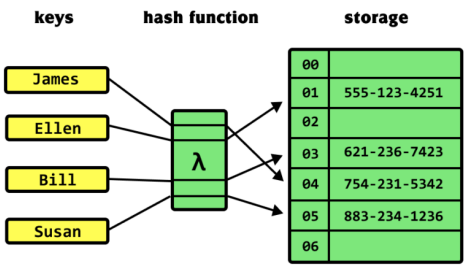
САДРЖАЈ

1 Увод

Хеш функцијом се назива било која математичка функција која се може користити за пресликавање података прооизвољне дужине у вредности фиксне дужине. Улазну вредност хеш функција називамо *порука, улазна порука или улазни подаци* (engl. message), а излазну *хеш, хеш вредност или дигест* (engl. digest). Ове вредности се најчешће користе за индексирање табела фиксне дужине, које се називају *хеш табеле* (слика 1).

Криптографске хеш функције се генерално користе на два начина:

- **Као споредни алат** - за стандардизацију тестирања других криптографских компонената, како би се осигурала безбедност. У овом сценарију такође служе као "izvor"случајности у криптографски сигурним псеудо-насумичним генераторима бројева.
- **Самостално** - Често се користе за верификацију интегритета података који су претходно прошли кроз шумовите и небезбедне комуникационе канале.



Слика 1: Хеш табела

2 Појмови важни за хеш функције

Дефиниција 1. *Хеш функцијом називамо функцију* $h : A \to B$*, где је* $A = \{a \in \{0,1\}^j, j \in \mathbb{N}\}$ *скуп свих битовних секвенци произвољне дужине* j *и* $B = \{0,1\}^k$ *скуп свих битовних секвенци дужине* k*.*

2.1 Безбедносни појмови

У криптографским околностима, хеш функције су дизајниране да испуне 3 основна безбедносна појма:

1. **Отпорност на прву претслику (FPR)** - хеш функција $h : A \to B$ је таква да је за свако $d \in B$ неизводљиво[1] одредити било које $m \in A$ тд. $h(m) = d$.
2. **Отпорност на другу претслику (SPR)** - хеш функција $h : A \to B$ је таква да је за свако $m \in A$ неизводљиво одредити било које $m' \in A$ тд. $h(m) = h(m')$ и $m \neq m'$.
3. **Отпорност на колизије** - хеш функција $h : A \to B$ је таква да је неизводљиво одредити неко $m \neq m' \in A$ td. $h(m) = h(m')$.

Својство	**Математички циљ**	**Сложеност**
FPR	За дато d, наћи m тако да је $h(m) = d$	2^k
SPR	За дато m, наћи $m' \neq m$ тако да је $h(m) = h(m')$	2^k
Отпорност на колизије	Наћи било која два различита улаза m, m' тако да је $h(m) = h(m')$	$2^{k/2}$

Табела 1: Упоредни приказ основних безбедносних својстава хеш функција

2.2 *Random oracle* функција

Тзв. *random oracle* функција је теоријски идеална хеш функција. Објаснимо принцип њеног функционисања. Када се *random oracle* функција $R : A \to B$ позива за поруку $m \in A$, она прво проверава да ли је већ била позвана за то конкретно m (функција није дефинисана за неко m док се не позове $R(m)$). Ако није, функција бира савршено насумично $d \in B$ и чува информацију да је m коришћено као улаз функције и да је генерисани хеш био d. Уколико је функција раније већ видела m, она ће вратити исто d као први пут. *Random oracle* функција задовољава сва три безбедносна појма из одељка 2.1, као и бројне друге. Функција је екстремно рачунарски интензивна и практично неизводљива у стварности. Такође, доказано је да ниједна процедурална хеш функција не може савршено имитирати насумично и безбедно понашање *random oracle* функције.

3 Универзалне фамилије хеш функција

Размотримо колекције хеш функија које се називају *фамилије*. Свака функција у фамилији хеш функције има исти домен и кодомен. Функције често имају исту структуру и разликују се једино у константама.

Дефиниција 2. *$H : A \to B$ је **универзална** фамилија хеш функција ако за свако $x \neq y \in A$ важи $P_{h \in H}(h(x) = h(y)) = \frac{1}{|B|}$, где P означава вероватноћу. Такође, $H : A \to B$ је **ϵ-скоро-универзална** фамилија хеш функција ако за свако $x \neq y \in A$ важи $P_{h \in H}(h(x) = h(y)) \leq \epsilon$.*

Дефиниција 3. *Нека је A Абелова група и $-$ операција одузимања у групи A. $H : A \to B$ је **Δ-универзална** фамилија хеш функција ако за свако $x \neq y \in A$ и свако $b \in B$ важи $P_{h \in H}(h(x) - h(y) = b) = \frac{1}{|B|}$. Такође, $H : A \to B$ је **ϵ-скоро-Δ универзална** фамилија хеш функција ако за свако $x \neq y \in A$ и свако $b \in B$ важи $P_{h \in H}(h(x) - h(y) = b) \leq \epsilon$.*

Дефиниција 4. *$H : A \to B$ је **снажно универзална** фамилија хеш функција ако за свако $x \neq y \in A$ и свако $r, s \in B$ важи $P_{h \in H}(h(x) = r, h(y) = s) = \frac{1}{|B|^2}$. Такође, $H : A \to B$ је **ϵ-скоро-снажно универзална** фамилија хеш функција ако за свако $x \neq y \in A$ и свако $r, s \in B$ важи $P_{h \in H}(h(x) = r, h(y) = s) \leq \frac{\epsilon}{|B|}$.*

[1] Неизводљивост задатка значи да би противнику који би га покушао била потребна нереална рачунарска снага, нереална рачунарска меморија или нереалан математички увид како би га извршио.

Лема 1. *За сваку фамилију $H : A \to B$ хеш функција са коначним A, постоје $x, y \in A$ тд. $P_{h \in H}(h(x) = h(y)) > \frac{1}{|B|} - \frac{1}{|A|}$.*

Теорема 1. *Нека $x \in A, S$ и нека x припада неком подскупу од A. Нека је h насумично изабрана функција из универзалне фамилије функција $H : A \to B$ Тада $P_{h \in H}(h(x) \in h(S)) \leq \frac{|S|}{|B|}$, где је $h(S)$ слика од S кроз h.*

4 MMH32 функција и примене

Једна од честих примена хеш функција је стримовање видеа. Хеш функције осигуравају интегритет података током преноса, омогућавајући детекцију порука које су модификоване или оштећене. Једна од ефикасних хеш функција која се користи за ово је MMH_{32} функција.

Дефиниција 5. *Нека је p прост број већи од 2^{32}. За поруку m која се састоји од l блокова од по 32 бита, $m = (m_1, m_2, \ldots, m_l)$, дефинишемо MMH_{32} хеш функцију као:*

$$MMH_{32}(m) = \left(\sum_{i=1}^{l} m_i \cdot a_i \right) \mod p$$

где су $a_1, a_2, \ldots, a_l$ насумично изабрани коефицијенти из скупа $\{0, 1, \ldots, p-1\}$.

5 Закључак

Криптографске хеш функције представљају један од фундаменталних стубова савремене информационе безбедности. Као што је кроз рад приказано, њихова моћ не лежи само у способности компресије података, већ у ригорозним математичким својствима која онемогућавају реверзибилно инжењерство и неовлашћене модификације садржаја.

Иако је теоријски идеал у виду random oracle функције практично недостижан, развој универзалних фамилија хеш функција омогућио је креирање алгоритама који нуде оптималан баланс између рачунарске ефикасности и математички доказиве сигурности. Анализа MMH_{32} функције показала је како се дискретна математика и теорија бројева успешно примењују у решавању реалних проблема, попут обезбеђивања интегритета података у системима за пренос мултимедијалног садржаја.

5.1 Будућност

У будућности, са развојем квантног рачунарства, значај математичке анализе хеш функција ће само расти, јер ће се тражити нови алгоритми отпорни на напредне методе криптоанализе, чиме ова тема остаје у самом центру интересовања како теоријске компјутерске науке, тако и практичне криптографије.