سیستم های اثباتی دانایی- صفر

به طور کلی در این پژوهش به تعریف مفهوم سیستم های اثباتی دانایی_صفر[1]، ویژگی های یک اثبات معتبر ،معیار هایی که مزایا و معایب سیستم اثباتی به وسیله آن ها سنجیده میشود و نحوه کلی کارکرد دو سیستم اثباتی بخصوص اشاره شد.

به طور کلی سیستم های اثباتی دانایی_صفر سیستم هایی هستند که به ما کمک میکنند تا اثبات کنیم از مقدار بخصوصی اطلاع داریم بدون این که آن مقدار را فاش کنیم. به طور مثال میتوان به پروتکل فیات-شمیر[2] اشاره کرد که به وسیله آن میتوانستیم اثبات کنیم که از مقدار ریشه یک عدد مربع کامل اطلاع داریم بدون این که آن مقدار را فاش کنیم.

هر اثبات دانایی_صفر دارای سه ویژگی است که اگر هرسه آن ها را دارا باشد، اثبات معتبر محسوب میشود. این سه ویژگی عبارتند از:

تمامیت[3]: اگر عبارت ما درست باشد یعنی ما واقعا مقدار متغیر مورد نظر را بدانیم، بتوانیم برای هر مقداری اثبات کنیم که آن مقدار را میدانیم.

صحت[4]: اگر عبارت ما نادرست باشد و ما مقدار متغیر را نداشته باشیم به هیچ عنوان نتوانیم با استفاده از سیستم اثباتی، اثبات کنیم که آن مقدار را داریم.

دانایی- صفر: نباید در هنگام اثبات هیچ اطلاعات اضافی فاش شود.

1: Zero-Knowledge 2: Fiat-Shamir 3: Completeness 4: Soundness

سیستم های متنوعی برای اثبات دانایی با دانایی- صفر وجود دارند که از معروف ترین آن ها میتوان به بولتپروف[1] ها، ز.ک.اسنارک[2] ها، استارک[3] ها و سیگما- پروتکل[4] ها اشاره کرد. هرکدام از این سیستم ها با توجه به استفاده ای که از آن ها صورت میگیرد مزایا و معایبی دارند که با استفاده از معیار های خاصی سنجیده میشوند. یکی از این معیار ها اندازه اثبات میباشد که هرچه کوتاه تر باشد، عملیات اثبات سریعتر انجام میپذیرد. دو معیار دیگر محاسبات سمت اثبات کننده و تایید کننده میباشند که در هربار اثبات توسط دوطرف صورت میپذیرد. معیار اخر راه اندازی اولیه میباشد که در بعضی از سیستم های لازم است و درواقع به محاسبات اولیه ی گاها" هزینه بری گفته میشود که در ابتدای راه اندازی سیستم باید توسط شخص یا سیستم مورد اعتمادی صورت پذیرد.

بولتپروف ها: به طور خلاصه با استفاده از این سیستم های اثباتی میتوان اثبات کرد که یک عدد یا بردار در بازه بخصوصی قرار دارد. به طور مثال اگر عدد 5 را در نظر بگیریم، میدانیم در مبنای دو به صورت 101 نوشته میشود پس بدیهی است که برای نشان دادن این عدد به صورت باینری حداقل به سه بیت نیاز داریم. حال اگر اعلام کنیم برای نشان دادن عددی به سه بیت نیاز داریم پس اثبات کرده ایم این عدد در بازه ی [0, 8) قرار دارد چون تمام اعدادی که میتوان با سه بیت نشان داد در این بازه قرار دارند.

1: Bullet proof 2: ZK-SNARK 3: STARK 4: Σ-protocol

ز.ک.اسنارک ها: سیستم های اثباتی غیر تعاملی اثبات_کوتاه دانایی_صفر هستند که به وسیله آن ها میتوان اعتبار یک چند جمله ای را ارزیابی کرد.

برای بررسی نحوه کارکرد ز.ک.اسنارک ها مسئله زیر را در نظر بگیرید:

فرض کنید آلیس یک چند جمله مانند $P(X)=a_0+a_1\cdot X+a_2\cdot X^2+...+a_d.X^d$ داشته باشد و باب نقطه دلخواه s را به صورت تصادفی از میدان Fp انتخاب کرده باشد (به طوری که p اول باشد) حال باب میخواهد مقدار P(s) را بداند بدون این که s را افشا کند یا p(x) را از عالیس بگیرد. برای حل این مسئله به تابعی مانند E(x) با شرایط زیر نیازمندیم.

- برای هر x اگر E(x) را داشته باشیم نتوان به راحتی x را پیدا کرد.
- برای هر ورودی خروجی متفاوت داشته باشیم.
- برای a, E(x), E(y) داده شده به راحتی بتوان E(ax+y) را محاسبه نمود.

حال باب میتواند مقادیر $E(1), E(s), ..., E(s^d)$ را با استفاده از یک تابع دلخواه با شریط گفته شده محاسبه کند و برای آلیس بفرستد تا آلیس بتواند این مقادیر را در چندجمله ای خود جایگذاری کند. به راحتی ثابت میشود مقدار محاسبه شده توسط آلیس برابر مقدار E(P(s)) است که آن را برای باب میفرستد.

سوالی که در این جا پیش میاید این است که باب چگونه میتواند مطمئن باشد عددی که توسط آلیس برای او فرستاده شده، همان مقداری است که از چندجمله ای به دست آمده.

برای جواب دادن به این سوال از لمی به نام لم شوارتز- زیپل[1] استفاده میکنیم که بیان میکند: " چند جمله ای های مختلف در بیشتر نقاط مقدار متفاوتی دارند. " به عبارت دیگر اگر فرد اثبات کننده به جای مقدار محاسبه شده در چندجمله ای عدی تصادفی به ما دهد به احتمال خیلی زیاد با مقدار محاسبه شده در چند جمله ای برابر نیست.

حال با دانستن این نکته باب، یک عدد تصادفی مانند a را از F^*_p که اعضای غیر صفر F_p هستند انتخاب میکند و علاوه بر مقادیر $E(1),E(s),\dots,E(s^d)$ مقادیر $E(a1),E(as),\dots,E(as^d)$ را نیز محاسبه کرده و برای آلیس میفرستد.

سپس آلیس مقادیر $A = E(P(s))$ و $B = E(P(\underline{S}))$ را محاسبه کرده و آن ها را برای باب میفرستد. پس از آن باب بررسی میکند که $B = a \cdot A$ باشد و اگر اعداد حاصل از یک چندجمله ای به دست آمده باشد پس این تساوی باید برقرار باشد.

با استفاده از این روش، اثبات کننده به راحتی میتواند اعتبار یک چند جمله ای را در نقطه ای که برای او نامشخص است، اثبات کند که مبنای کار بسیاری از پروتکل های ز.ک. اسنارک میباشد.

به طور کلی اثبات های دانایی- صفر کمتر از بیست سال است که ابداع شده اند و همچنان تحقیقات و مطالعات زیادی درمورد این سیستم ها صورت میگیرد که در این مطلب به مبنای کار دو مورد از این سیستم ها اشاره شد.

1: Schwartz-Zippel Lemma

1: Schwartz-Zippel Lemma