پیوست‌های یادداشت ساختار پول دیجیتال بین کوین

پیوست یکم: تابع چکیده ساز SHA۲۵۶

توابع چکیده ساز یا hash نقشی اساسی در ایجاد امنیت و اصالت در شبکه های مبتنی بر زنجیره‌بلوک ایفا میکند. این توابع به صورت یکطرفه ورودی را که در هر اندازه ای میتواند باشد، به یک خروجی با اندازه مشخص تبدیل میکند. به عبارتی دیگر ماشینی است که از روی هر متن و داده ای با هر اندازه ای را به یک عبارت با طول مشخص رسید. این خروجی را هش ورودی مینامیم.

توابع چکیده ساز خوب بایستی چند شرط داشته باشند:

۱- بایستی هرکس در هر زمانی که از تابع برای چکیده کردن یک عبارت خاص استفاده میکند به یک عبارت مشخص و یکسان برسد. به عبارت دیگر این تابع نباید حاوی عناصری تصادفی یا هر ورودی دیگری به جز متن ورودی باشد و از اینرو یک تابع متعین[۱] است.
۲- خروجی باید شبه تصادفی باشد و هر بیت آن به تمام متن وابسته باشد.
۳- به صورت محاسباتی نتوان از چکیده به متن ورودی رسید(یکطرفه بودن)
۴- نتوان دو ورودی با چکیده یکسان یافت.(نبود احتمال تصادم)
۵- از نظر محاسباتی سریع باشد.

از توابع هش برای تامین یکپارچگی پیام، امضا و ... میتوان استفاده کرد. در شبکه های مبتنی بر زنجیره‌بلوک همانگونه که پیش از این اشاره شد در استخراج نیز استفاده میشود.

تابع هش مورد استفاده در سیستم بیتکوین SHA۲۵۶ است که ورودی آن هر اندازه ای میتواند باشد و هش آن ۲۵۶ بیت یا ۳۲ بایت است. الگوریتم آن مختصرا به این صورت است:

۱- اگر بخواهیم الگوریتم را به یک ماشین باینری تشبیه کنیم رجیسترهای آن ۳۲ بیتی هستند. ۸ رجیستر خروجی H، هشت رجیستر زنجیره ای C، ۶۴رجیستر K و ۶۴ رجیستر W در این ماشین وجود دارند. منظور از کلمه نیز کلمه ۳۲بیتی است. رجیسترهای خروجی در پایان الگوریتم نشاندهنده خروجی هستند. در آغاز رجیسترهای H و K مطابق استاندارد الگوریتم مقداردهی اولیه میشوند.
۲- به پیام ورودی یک بیت ۱ و K بیت صفر و متغیر ۶۴ بیتی L که طول پیام را نشان میدهد اضافه میکنیم به نحوی که L+۱+K+۶۴ مضرب ۵۱۲ باشد و ۰≤K<۵۱۲

[۱] Deterministic Function

۳- پیام را به قطعات۵۱۲ بیتی (هر قطعه ۱۶ کلمه) تقسیم میکنیم.

۴- برای هر قطعه باید عمل زیر را انجام دهیم:

۴-۱- W را با توجه به قطعه پیام مقداردهی میکنیم. ۱۶ رجیستر اول را مستقیما از قطعه کپی میکنیم و بقیه را با طی عملیاتی که مبتنی بر عملهای بیتی نظیر XOR و شیفت و عمل جمع است از روی ۱۶ رجیستر اول میسازیم

۴-۲-هشت رجیستر C را از روی رجیسترهای H مقدار دهی اولیه میکنیم.

۴-۳- عمل زیر را ۶۴ دور انجام میدهیم:

۴-۳-۱- دو مقدار موقت temp۱,temp۲ طی عملیاتی که مبتنی بر عملهای بیتی نظیر XOR و شیفت و عمل جمع است از روی K و W و C میسازیم.

۴-۳-۲- رجیسترهای C را به صورن کلمه ای به چپ شیفت میدهیم

C[i]=C[i-۱] i=۷ downto ۱

۴-۳-۳- دو رجیستر خاص C را اینگونه مقدار میدهیم:

C[۰]=temp۱+temp۲ , C[۴]=C[۴]+temp۲

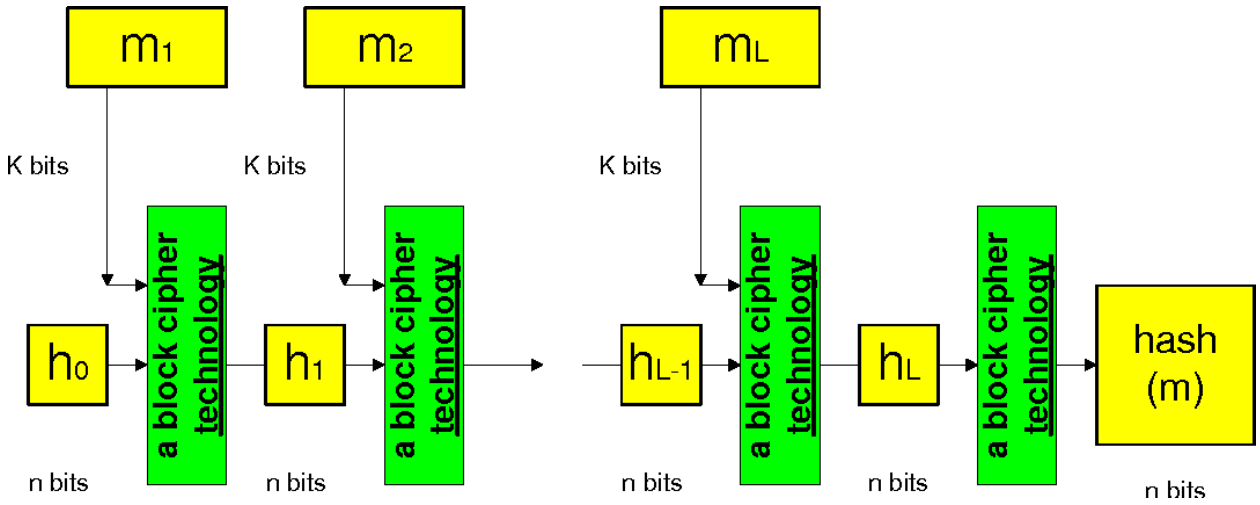
۴-۴- پس از انجام عمل بند پیش و ۶۴ بار تغییر در زنجیره رجیستر C مقدار آنها را به رجیستر خروجی H اضافه میکنیم(H=H+C) و کار ما با قطعه پیام به پایان میرسد.

۵- پس از طی شدن مراحل بند ۴ برای همه قطعات(که در هر اجرا مقدار رجیسترهای H یک بار تغییر میکند) مقدار H را به عنوان خروجی و هش انتخاب میکنیم.

الگوریتمی که در بالا ذکر کردیم تفریبا کامل است، ولی از بیان برخی عبارات پیچیده تر آن اجتناب کردیم. این الگوریتم به صورت کامل در [۷] ذکر شده است.

این الگوریتم و الگوریتمهای مشابه که آنها را میتوان الگوریتم چکیده ساز مبتنی بر رمزنگاری دانست در واقع از یک رمزکننده قالبی[۲] بهره میبرند. با این تفاوت که الزامی به برگشت‌پذیر بودن و قابل رمزگشایی بودن رمزکننده مذکور نیست. از این لحاظ عملکرد تابع هش به این صورت است که ابتدائا پیام را گسترش میدهد تا به اندازه قالب رمز کننده بخشپذیر شود و آنرا بتوان به قطعات یکسان شکست. اندازه قالب رمزکننده در SHA۲۵۶ برابر ۵۱۲ بیت است. سپس با استفاده از یک کلید ثابت و مقدار H و در طی یک عملیات ۶۴ دوری به یک مقدار رمز شده ۲۵۶ بیتی میرسد. مقدار رمز شده هر بار با H جمع میشود و نهایتا H به عنوان خروجی مشخص میشود.

[۲] Block cipher

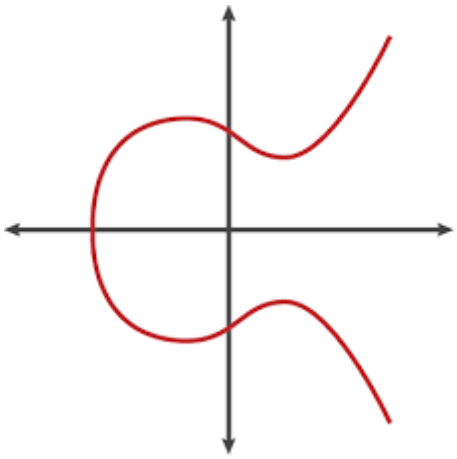


شکل ۶) تابع چکیده ساز مبتنی بر رمز قالبی

پیوست دوم: رمزنگاری خم‌های بیضوی

تایید اصالت یک تراکنش و تعلق آن به خرج کننده از طریق امضا صورت میگیرد. امضا در سیستم بیت‌کوینبه روش منحنیهای بیضوی صورت میپذیرد. در این بخش توضیح مختصری درباره نحوه امضا داده میشود.

منحنی بیضوی یک منحنی با معادله مشخصه $y^2=x^3+ax+b$ است به صورت زیر است:



شکل ۷) یک منحنی بیضوی

این نمودار را میتوان در میدانهای متناهی نیز تعریف کرد. برای مثال منحنی بیضوی استفاده شده در بیتکوین به صورت زیر است

$$y^2 = (x^3 + 7) \text{over} (\mathbb{F}_p)$$

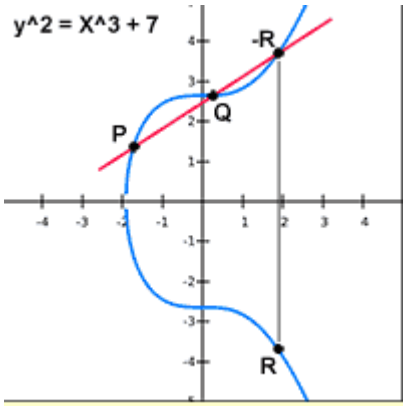
or

$$y^2 \mod p = (x^3 + 7) \mod p$$

$$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$$

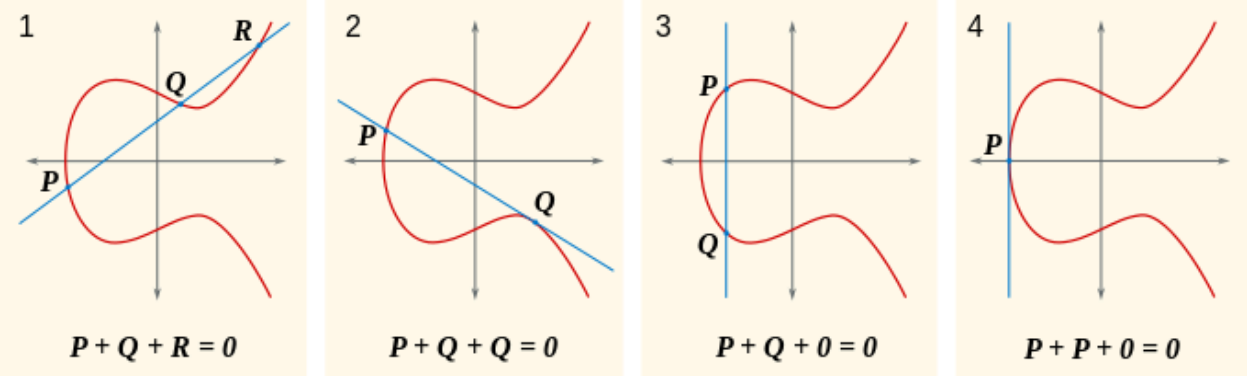
به عبارت دیگر ضرب و جمع و... در آن به پیمانه عدد اول p انجام میشود. در منحنی بیضوی میتوان بین نقاط منحنی عمل جمع تعریف کرد. این جمع به این صورت است دو نقطه منحنی را با خطی به هم وصل میکنیم. این خط منحنی را در نقطه سومی قطع خواهد کرد. قرینه این نقطه نسبت به محور افقی حاصل جمع دو نقطه آغازین است. واضح است که این جمع خاصیت جابجایی دارد و نقطه خنثی آن در بی نهایت است. به همین دلیل میتوان آنرا یک گروه جبری تلقی کرد.

P+(Q+R)=(P+Q)+R P+∞=P P+Q=Q+P



شکل ۸) عمل جمع در منحنی بیضوی بیتکوین

در این شکل به برخی از اشکال جمع روی منحنی بیضوی اشاره شده است. منظور از ۰ عضو خنثی یا همان بینهایت است



شکل ۹) جمعهای خاص در منحنی بیضوی

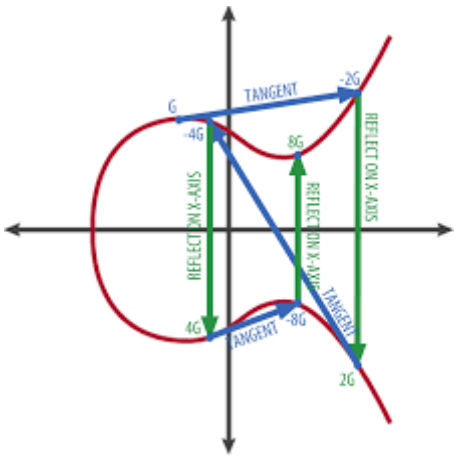
علاوه بر این در این گروه یک نوع ضرب اسکالر تعریف میشود که حاصل ضرب عددی طبیعی در یکی از نقاط منحنی است. در این ضرب kP به سادگی برابر با k بار جمع کردن P با خودش تعریف میشود.

Q=kP=P+P+P+…..+P (k times)

در یک منحنی بیضوی تحت میدان متناهی برای هر عضو منحنی نظیر P عدد m وجود دارد به نحوی که mP=∞ این عدد را مرتبه P در منحنی میگوییم. بزرگترین مرتبه ممکن در یک منحنی بیضوی را مرتبه منحنی میگوییم

اثبات میشود که مرتبه منحنی تعریف شده ذیل میدان متناهی GF(p) به صورت n=p+۱-t قابل نوشتن است که در آن $|t| < ۲\sqrt{p}$ که به قضیه هاسه موسوم است. بدین ترتیب میتوان دریافت که در هر منحنی بیضوی تعریف شده در یک میدان متناهی میتوان عضو مولدی یافت که مرتبه آن نزدیک به اندازه میدان متناهی باشد. به همین صورت میتوانیم بگوییم که مرتبه منحنی بیضوی بیتکوین عددی ۲۵۶ بیتی است و منحنی بیضوی آن

تا $۲^{۲۵۵}$ نقطه قابل استفاده دارد. استفاده از منحنیهای بیضوی در امضا و رمزنگاری مستلزم محاسبه کردن جمع و ضرب اسکالر است. جمع را میشود با توصیف هندسی ای که ذکر کردیم انجام داد، ولی با این تفاوت که به جای ضرب و تقسیم و جمع و تفریق عادی از معادلهایشان در میدانهای متناهی استفاده شود. جهت ضرب اسکالر Q=mP، میتوان اسکالر را بر مبنای دو و به صورت مجموع توانهای دو نوشت. همچنین به صورت پیشینی ۲P و ۴P و ۸P و... را محاسبه کرد و mP را به صورت مجموع چند نقطه منحنی محاسبه کرد.



شکل ۱۰) نقطه مولد و ضرب اسکالر توانهای دو در آن

مسئله لگاریتم گسسته بر روی منحنی بیضوی

مسئله به این شرح است که فرض کنید Q=kP که Q,P نقاطی روی منحنی بیضوی باشند. چگونه با دانستن آنها به k برسیم؟ این مسئله دشوار است و بهترین الگوریتم حل آن زمانی در مرتبه $\sqrt{n}$ نیاز دارد که n مرتبه P در منحنی است. این مسئله از نظر دشواری شبیه مسئله لگاریتم گسسته است که الگوریتم رمز نامتقارن الجمال بر اساس آن ساخته شده است.

امنیت الگوریتمهای رمزنگاری و امضای منحنی بیضوی به سختی حل این مسئله برمیگردد. P را طوری انتخاب میکنند که مرتبه آن با مرتبه منحنی یکی باشد و بیشترین مرتبه ممکن را داشته باشد. P را نقطه مولد مینامیم و به طور عمومی منتشر میکنیم. سپس $Q=d_aP$ را حساب میکنند و Q را به عنوان کلید عمومی منتشر میکنند و d_a را بعنوان کلید خصوصی در نزد خود نگه میدارند و کسی نمیتواند از Q به d_a برسد. بخاطر اینکه افزایش دشواری با جذر n مرتبط است برای حصول ۱۲۸ بیت امنیت کلید خصوصی و مطابق با آن p , n بایستی کلید طولی به اندازه ۲۵۶ داشته باشد.

طریقه امضا کردن و چک کردن امضا قدری پیچیدگی دارد و باید دقت کرد محاسبات آن در GF(n) صورت میپذیرد. همچنین باید دقت کرد که منحنی بیضوی طوری انتخاب شود که n هم عدد اول شود. مثلا در منحنی بیضوی بیتکوین داریم:

n = ۰xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE٦AF٤٨A٠٣BBFD٢٥E٨CD٠٣٦٤١٤١

طریقه امضا:

۱- پیام را هش کنید. e=HASH(m)

۲- ۲۵۶ بیت(یا به طور کلیتر تعداد بیتهای n مرتبه منحنی) از سمت چپ e بردارید و در z قرار دهید.

۳- عدد k را به طور مخفی انتخاب کنید ۰<k<n

۴- X=kG را به روش ضرب اسکالر منحنی بیضوی تولید کنید. $X=(r,y_1)$

۵- اگر r=۰ برگرد به ۳

۶- $s= k^{-1}(z+rd_a) \bmod n$ را حساب کنید. d_a کلید خصوصی است و k^{-1} معکوس k به پیمانه n است به نحوی که $k.k^{-1}=1 \bmod n$ اگر s=۰ برگرد به ۳

۷- (r,s) را به عنوان امضا منتشر کنید.

باید دقت کرد که نه تنها k باید مخفی بماند بلکه هربار و در امضای متن متفاوت باید عوض شود. چرا که استفاده از kیکسان برای دو امضا سبب میشود دشمن به کلید خصوصی ما پی ببرد.

طریقه چک کردن امضا:

برای چک کردن امضا به G و Q کلید عمومی، n مرتبه منحنی m پیام و منحنی بیضوی و همچنین امضا دسترسی داریم.

۱- چک کنید که ۰<r,s<n

۲- پیام را هش کنید. e=HASH(m)

۳- ۲۵۶ بیت(یا به طور کلیتر تعداد بیتهای n مرتبه منحنی) از سمت چپ e بردارید و در z قرار دهید.

۴- مقادیر $u_1=zs^{-1} \bmod n$ و $u_2=rs^{-1} \bmod n$ را حساب کنید

۵- با استفاده از مفهوم جمع و ضرب اسکالر در منحنی بیضوی حساب کنید: $X=u_1\times G+u_2\times Q$ که $X=(x_1,y_1)$

۶- اگر $r=x1 \bmod n$ امضا تایید میشود و در غیر این صورت رد میشود.

اثبات: جهت اثبات فرض میکنیم امضا درست صورت پذیرفته و تا مرحله ۵ پیشرفته ایم. با توجه به اینکه $Q=d_aG$ داریم:

$X=(zs^{-1} \bmod n)\times G+(rs^{-1} \bmod n).d_a\times G$

$X=(zs^{-1}+rd_as^{-1} \bmod n)\times G=(s^{-1}(z+rd_a) \bmod n)\times G$

$X=((k^{-1}(z+rd_a))^{-1}(z+rd_a) \bmod n)\times G=(k(z+rd_a)^{-1}(z+rd_a) \bmod n)\times G$

$X=k\times G=(r,y_1)$

بنابرین اگر همان مقادیر مبدا را در معادلات قرار دهیم r دوباره ساخته خواهد شد و امضا مطابقت دارد در غیر این صورت امضا مطابق نخواهد بود و رد میشود.

از مزایای امضای مبتنی بر منحنی بیضوی طول کلید و نتیجا پیچیدگی کمتر به نسبت RSA برای امنیت مشابه است. از دیگر سو میتوان با یک چارچوب و منحنی بیضوی مشخص به زوج کلید عمومی و خصوصی تولید کرد. در حالی که در RSA اگر نخواهیم ساختار را تغییر دهیم باید به مرجعیت یک مرکز برای تولید کلید عمومی-خصوصی تن دهیم. همین ویژگی این نحوه امضا را برای بیت‌کوینکه حالتی توزیع شده و مرکز زدایی شده دارد مناسب میسازد.

منابع:

[۱] https://coiniran.com

[۲] https://en.bitcoin.it/wiki/Main_Page

[۳] Nakamoto, Satoshi. "Re: Bitcoin P۲P e-cash paper." Email posted to listserv ۹ (۲۰۰۸): ۰۴.

[۴] https://bitnodes.earn.com/

[۵] Antonopoulos, Andreas M. *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.", ۲۰۱٤.

[٦] Antonopoulos, Andreas M. *Mastering Bitcoin: Programming the Open Blockchain*. " O'Reilly Media, Inc.", ۲۰۱۷.

[۷] https://en.wikipedia.org/wiki/SHA-۲

[۸] https://en.bitcoin.it/wiki/Secp۲۵٦k۱

[۹] Simple Tutorial on Elliptic Curve Cryptography: http://www.eis.mdx.ac.uk/staffpages/m_cheng/link/ecc_simple.pdf

[۱۰] https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm