


دانشکده‌ی علوم ریاضی

مقدمه‌ای پیشرفته بر رمزنگاری ۲۸ آبان ۱۳۹۱

جلسه‌ی ۱۸: اثبات دانش-صفر

مدرس: شهرام خزائی *نگارنده: سید کاوه حسینی*

در جلسه‌ی پیش در مورد سامانه‌های اثبات تعاملی [۱] بحث شد. در این جلسه مفهوم جدیدی با نام اثبات دانش-صفر[۲] مطرح خواهد شد.

۱ مقدمه

در رمزنگاری یک *اثبات دانش-صفر* یا *پروتکل دانش-صفر* به روشی تعاملی اطلاق می شود که در آن یک پارتی می خواهد درستی یک گزاره را برای پارتی دیگر ثابت کند با این محدودیت که پارتی دوم هیچ گونه دانشی فراتر از اطلاع از درستی گزاره‌ی مذکور کسب نکند.

تعریف ۱ *سامانه‌ی رمز متقارن* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *دارای امنیت (معنایی) دانش-صفر است اگر یک شبیه‌ساز احتمالاتی با زمان چند جمله‌ای* $\mathcal{S}$ *وجود داشته باشد که برای هر پیام* $m \in \{0,1\}^n$ *گردایه های زیر از لحاظ محاسباتی غیر قابل تمایز باشند:*

- $\{k \leftarrow \mathsf{Gen}(1^n) : \mathsf{Enc}_k(m)\}$
- $\{\mathcal{S}(1^n)\}$

تعریف مشابهی بر اساس وجود حمله‌کننده به همراه یک پارامتر اضافی ارایه شده است.

تعریف ۲ *سامانه‌ی رمز متقارن* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *دارای امنیت (معنایی) دانش-صفر است اگر برای هر حمله کننده ی چندجمله ای* $\mathcal{A}$ *و هر* $z \in \{0,1\}^{p(n)}$ *گردایه‌های زیر از لحاظ محاسباتی غیر قابل تمایز باشند:*

- $\{k \leftarrow \mathsf{Gen}(1^n) : \mathcal{A}(\mathsf{Enc}_k(m), z)\}$
- $\{\mathcal{S}(1^n, z)\}$

تعریف ۳ *فرض کنید* (P,V) *یک اثبات تعاملی برای زبان* L *باشد. می‌گوییم* (P,V) *دانش-صفر کامل*[۳] *است اگر برای هر ماشین تعاملی احتمالاتی* V^* *با زمان اجرای چندجمله‌ای، یک شبیه‌ساز چندجمله‌ای احتمالاتی* $\mathcal{S}$ *وجود داشته باشد که برای هر* $x \in \{0,1\}^*$ *توزیع های زیر یکسان باشند:*

[۱] Interactive Proof Systems
[۲] Zero-Knowledge Proofs
[۳] Perfect Zero-Knowledge

- $\mathsf{view}^P_{V^*}\langle P(x) \leftrightarrow V^*(x)\rangle$
- $\mathcal{S}(x)$

که در اینجا $\mathsf{view}^P_{V^*}\langle P(x) \leftrightarrow V^*(x)\rangle$ *دنباله‌ی رشته‌های رد و بدل شده بین* V^* *و* P *است.*

تعریف بالا بسیار محدود کننده است و با این تعریف تنها زبانهای عضو کلاس BPP پروتکل دانش-صفر کامل خواهند داشت. تعریف را کمی ضعیف‌تر می‌کنیم با این هدف که کلاس بزرگتری از زبان‌ها را پوشش دهیم.

تعریف ۴ دانش-صفر کامل
فرض کنید (P,V) *یک اثبات تعاملی برای زبان* L *باشد. می گوییم* (P,V) *دانش-صفر کامل*[۴] *است اگر برای هر ماشین تعاملی احتمالاتی* V^* *با زمان اجرای چند جمله ای ، یک شبیه‌ساز چندجمله‌ای احتمالاتی* $\mathcal{S}$ *وجود داشته باشد که برای هر* $x \in \{0,1\}^*$ *دو شرط زیر برقرار باشند:*

۱. *(برای هر ورودی* x *)* شبیه‌ساز $\mathcal{S}$ *خروجی* $\perp$ *را با احتمال حداکثر* $\frac{1}{2}$ *تولید می کند.(با این مفهوم که* $\mathcal{S}$ *نتوانسته خروجی مطلوب را تولید کند.)*

۲. $\mathcal{S}^*(x)$ *را متغیر تصادفی* $\mathcal{S}$ *بگیرید با این شرط که* $S(x) \neq \perp$ *.* (به عبارتی $\Pr[\mathcal{S}^*(x) = \alpha] = \Pr[\mathcal{S}(x) = \alpha | \mathcal{S}(x) \neq \perp]$ *برای هر* $\alpha \in \{0,1\}^*$ *). در این صورت متغیرهای تصادفی زیر هم‌توزیع هستند.*

- $\mathsf{view}^P_{V^*}\langle P(x) \leftrightarrow V^*(x)\rangle$ (*خروجی حاصل از تعامل بین* P *و* V^*)
- $\mathcal{S}^*(x)$

۲ مسئله‌ی هم‌ریختی گراف‌ها

تعریف ۵ *گراف‌های* G_1 *و* G_2 *را یکریخت می نامیم و با* $G_1 \simeq G_2$ *نشان می دهیم اگر جایگشتی مثل* π *از رئوس* G_1 *وجود داشته باشد به طوری که* $\pi(G_1) = G_2$ *.*

تعریف ۶ *زبان همه زوج گراف های یکریخت را که به شکل زیر تعریف می شود در نظر بگیرید.*

$$GI = \{(G_0, G_1) : G_0 \simeq G_1\}$$

می خواهیم یک پروتکل دانش-صفر کامل برای این زبان ارایه دهیم.
ورودی $x = (G_0, G_1)$ است که $|G_0| = |G_1| = n$.
جایگشت σ را طوری بگیرید که $G_1 = \sigma(G_0)$ توجه کنید که P بایستی به روشی بتواند V را قانع کند که این دو گراف هم ریخت هستند ولی V نباید هیچ گونه دانشی در مورد σ کسب کند.
پروتکل به شرح زیر است.

۱. P یک جایگشت تصادفی π را انتخاب کرده و $H = \pi(G_0)$ را به V می فرستد.

۲. V یک بیت تصادفی b را انتخاب کرده و آن را به V می فرستد.

[۴] Zero-Knowledge Proof

۳. اگر $b = ۰$ که P همان π را می فرستد. در غیر اینصورت ، $\gamma = \pi \cdot \sigma^{-۱}$ را می فرستد.

۴. V خروجی ۱ را بر می گرداند اگر و تنها اگر $\gamma(G_b) = H$.

قضیه ۱ *پروتکل بالا برای زبان GI یک پروتکل تعاملی دانش-صفر کامل است.*

برهان. ابتدا تمامیت و درستی پروتکل را ثابت کرده سپس نشان می‌دهیم پروتکل دانش-صفر کامل است.

تمامیت

اگر $G_۰$ و $G_۱$ همریخت باشند، به وضوح V همواره خروجی ۱ را بر می‌گرداند.

درستی

اگر $G_۰$ و $G_۱$ همریخت نباشند، H ارسال شده از طرف P حداکثرمی تواند با یکی از $G_۰$ یا $G_۱$ همریخت باشد. فرض کنید G_i با H همریخت باشد. در این صورت با توجه به اینکه با احتمال $\frac{۱}{۲}$، $b \neq i$، احتمال شکست هر P حداقل $\frac{۱}{۲}$ خواهد بود.

دانش-صفر کامل

شبیه‌ساز $\mathcal{S}$ را معرفی می‌کنیم. سپس نشان می دهیم ویژگی‌های لازم را دارد.

$\mathcal{S}$ ورودی زیر را می‌گیرد، سپس الگوریتم زیر را اجرا می کند.

۱. یک بیت تصادفی b' و جایگشت تصادفی $\pi \in S_n$ را انتخاب کن.

۲. $H = \pi(G_{b'})$ را محاسبه کن.

۳. $V^*(x)$ را روی H شبیه سازی کن. خروجی حاصل از شبیه سازی $V^*(x)$ را b بگیرید.

۴. اگر $b = b'$ همان b را به عنوان خروجی برگردان، در غیر اینصورت $\perp$ را برگردان.

با توجه به استقلال b و b' ، احتمال $b = b'$ برابر $\frac{۱}{۲}$ است و لذا $\mathcal{S}$ با احتمال $\frac{۱}{۲}$ خروجی $\perp$ را برمی‌گراند. نشان می‌دهیم برای $x \in GI$، خروجی $\mathcal{S}$ اگر $\perp$ نباشد با خروجی $\langle P, V^* \rangle(x)$ هم توزیع است. توجه کنید که توزیع احتمال H و $\pi(G_۰)$ یکسان است. پس در حالت $b = b'$ توزیع احتمال $\mathcal{S}(x)$ و $\langle P, V^* \rangle(x)$ یکسان است.

■

این تعریف را می‌توان به طور مشابه برای دانش-صفر محاسباتی [۵] و دانش-صفر آماری [۶] ارایه داد.
کلاس زبان‌های دانش-صفر محاسباتی را با این تفاوت تعریف می‌کنیم که دو توزیع احتمال در تعریف مربوطه باید غیر قابل تشخیص باشند. این کلاس را با CZK نشان می دهیم. در تعریف کلاس دانش-صفر آماری که با SZK نشان می‌دهیم، فاصله ی آماری توزیع ها باید قابل اغماض باشد. می توان نشان داد که روابط زیر بین این کلاس‌ها برقرار است.

$$\mathsf{BPP} \subset \mathsf{PZK} \subseteq \mathsf{SZK} \subsetneq \mathsf{CZK}$$

تساوی SZK و PZK هنوز باز است.

[۵] Computational Zero-Knowledge
[۶] Statistical Zero-Knowledge