Pruebas de conocimiento cero

Andrea González Luis Mayo Carlos Acosta

11 de junio de 2017

Índice

1. Introducción

En nuestras experiencias tanto dentro como fuera del mundo académico, por lo general se nos exige que cualquier proposición comunicada al otro, sea sustentada con evidencias claramente expuestas como acompañamiento de nuestra declaración. A fin de inducir en ella un carácter de verdad, la defensa de nuestros enunciados debe apoyarse de argumentos que conserven la validez dentro del objetivo que perseguimos.

Pero, ¿qué ocurre cuando no podemos permitir que nuestra audiencia se entere de los detalles del camino que nos condujo al resultado que le presentamos?, ¿es posible mantener la confiabilidad, sin necesidad de proveer información más allá de la afirmación de que lo que decimos es verdad?

Sin cruzar apresuradamente al terreno de la magia o de la fe, consideremos primero la noción de las ***pruebas de conocimiento cero*** (ZPK[1]). Imaginemos que estamos solicitando un trabajo para una organización o empresa y es necesario que les convenzamos de nuestra valía, sin embargo toda la experiencia con la que contamos ha sido obtenida en los círculos del bajo mundo o la clandestinidad y no estamos en libertad de proporcionar un *curriculim vitae* o documento que demuestre nuestra competencia. En ese caso la empresa podría someternos a un periodo de prueba que consista en resolver problemas o tareas que atañen a nuestras habilidades, aún sin conocer el proceso que estamos llevando a cabo para ninguna de ellas -ya que no podemos revelar dichas técnicas por su naturaleza secreta-, entre más labores sean requeridas más certeza tendrán de aceptar nuestra solicitud de trabajo y menor probabilidad de que no estemos siendo honestos.

Así, en una prueba de conocimiento cero, si A (el "demostrador") busca probar a B (el "verificador") que una proposición X es verdadera, al término del proceso A estará completamente convencida de X, pero no habrá obtendido ningún nuevo conocimiento (barak []). De ahí el nombre, propuesto por primera vez en 1985 por los científicos de la computación Shafi Goldwasser, Silvio Micali, y Charles Rackoff en su artículo *La complejidad del conocimiento de los sistemas de demostración interactivos* [2], en el que definieron una nueva jerarquía de para las pruebas de conocimiento interactivas -de las que hablaremos más adelante-; concibieron además el concepto de *complejidad de conocimiento*[3] y presentaron el primer ejemplo de una prueba de conocimiento cero para un problema concreto. Sus esfuerzos en esta materia les valió a los tres autores un *premio Gödel* en 1993[4].

[1] Del inglés: *Zero Knowledge Proofs*

[2] Intento de traducción del inglés: *The knowledge complexity of interactive proof systems*

[3] Del inglés: *Knowledge complexity*, medida de la cantidad de conocimiento que el demostrador transfiere al verificador

[4] Premio anual otorgado por EATCS y la ACM SIGACT para artículos destacados en teoría de las ciencias de la computación. Lista de Ganadores del premio Gödel

1.1. Una pequeña historia

Estrictamente hablando, al contrario de una prueba matemática,

1.2. Características

2. Sistemas de Demostración Interactivos

La clase de complejidad *IP* [1]

3. Instancia

3.1. Protocolo de conocimiento cero para *logaritmo discreto*

[4] Sea $G = \langle g \rangle$ un grupo cíclico de orden q con un generador g, ambos q y g conocidos, y sea $x \in G$ un elemento arbitrario del grupo que tiene el logaritmo discreto $w = log_g(x)$. Tanto el probador P como el verificador V reciben como entrada a x, pero P recibe además a w.
El protocolo entre P y V se describe a continuación.

1. $P(x, w)$ elige aleatoriamente a un elemento $0 \leq r < q - 1$ y envia $z = g^r (\text{mod } q)$ a V.
2. $V(x)$ envia un bit $b \in \{0, 1\}$ aleatorio a P.
3. P responde con $a = r + b \cdot w \in Z_q$
4. V acepta si $g^a = z \cdot x^b (\text{mod } q)$

La idea básica es que si el bit $b = 1$, entonces P envia un número que parece aleatorio ($a = r + b \cdot x (\text{mod } q - 1)$) a V, pero V ya conoce $z = g^r (\text{mod } q)$ y sabe que $x = g^w$ por lo que puede multiplicar estos y compararlos con g^a.
En realidad, V solo puede ver a z y a y lo que sabe es que $a = log_g(z) + w$. Como ambos conocen s, pero el probador además conoce a w, entonces solo le queda demostrarle al verificador que también sabe $log_q(z)$.
Ahí es donde entra el bit aleatorio que envió V. Si $b = 0$, P solo envia $s = r$ de vuelta a V en el paso 3. V revisa que $z = g^r (\text{mod } q)$, es decir, $r = log_q(z)$. De este modo, dependiendo del valor de b, el verificador obtendrá r o a pero jamás ambas (ya que su diferencia es precisamente w). Por lo tanto V no obtiene ninguna información acerca de w.

3.2. Análisis

Veamos entonces que el protocolo satisfaga las tres propiedades de las pruebas de conocimiento cero.

- **Totalidad:**
  Si P y V actuan como está descrito en el protocolo, entonces tenemos que

$$g^a = g^{r+b\cdot w} = g^r \cdot (g^w)^b = z \cdot x^b$$

- **Solvencia:**
  Hay que notar que todas las $x \in G$ tiene logaritmo discreto, entonces no puede haber ningún probador deshonesto que engañe al verificador de que su declaración es cierta cuando sea falsa. Podríamos decir que el concepto de *solvencia* no es particularmente significativo en este caso.

- **Conocimiento cero:**
  Supongamos que existe un verificador engañoso V^*. Definimos entonces un simulador $mathcal S^{V^*}(x)$ del modo siguiente:

  1. Elige un bit aleatorio b y un elemento $a \in G$.
  2. Envia $z = g^a/x^b$ a V^* y recupera un bit de desafío b^*. Si V^* responde con un mensaje mal formado o aborta, solo muestra la salida de la vista hasta el momento.
  3. Si $b^* = b$, completa la vista usando a a como el último mensaje del probador, en caso contrario rebobina V^* y repite la simulación.

  Es relativamente fácil demostrar que S reproduce la vista de V^* hasta una distancia estadística insignificante ya que el valor de z calculado por S es estadísticamente independiente de su bit b, por lo tanto, tenemos que

$$Pr[b^* = b] = \frac{1}{2}$$

4. Conclusiones

Referencias

[1] Arora, S., Barak, B. *Computational complexity: a Modern Approach.* Beijing: World Publishing Corporation. 2012.

[2] Goldwasser, S., Micali, S., Rackoff, C. *The knowledge complexity of interactive proof-systems.* Proceedings of the seventeenth annual ACM symposium on Theory of computing - STOC 85. doi:10.1145/22145.22178. 1985.

[3] Quisquater, Jean-Jacques; Guillou, Louis C.; Berson, Thomas A. *How to Explain Zero-Knowledge Protocols to Your Children*. Advances in Cryptology - CRYPTO '89: Proceedings 435: 628-631. 1990.

[4] Peikert C, *Proofs of Knowledge* https://wiki.cc.gatech.edu/theory/images/5/54/Lec
Theoretical Foundations of Cryptography. Georgia Tech. 2010