Zero Knowledge Proofs

Seguridad informática

Hernán Guillermo Dulcey Morán

Cinvestav Tamaulipas

25 de Marzo de 2020

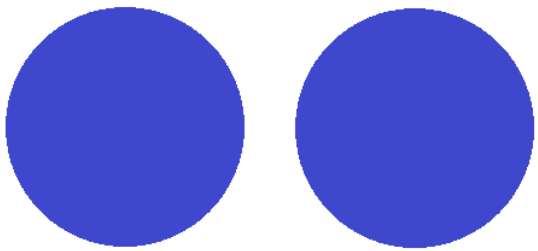
Contenido

Introducción

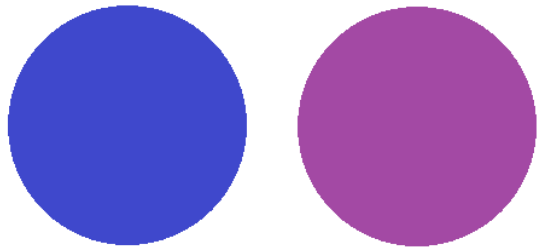
- ¿Es posible determinar la veracidad de una declaración sin conocer detalles sobre esta?
- ¿Es posible convencer a alguien que se conoce la contraseña, sin necesidad de revelar la contraseña?

Daltonismo

- Contemplemos el siguiente escenario:



Daltonico

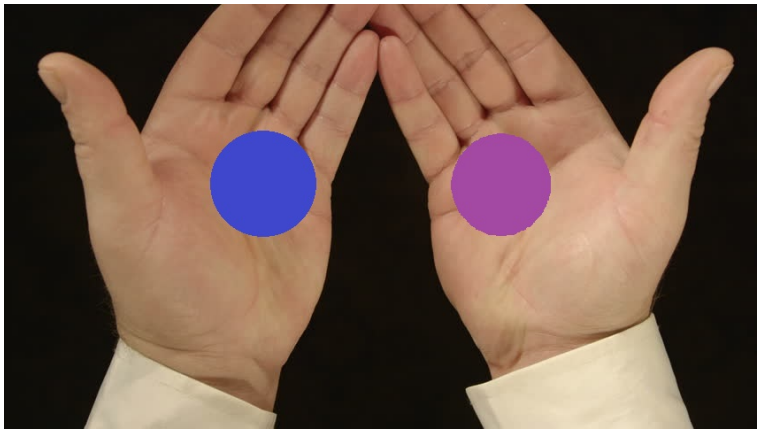


Normal

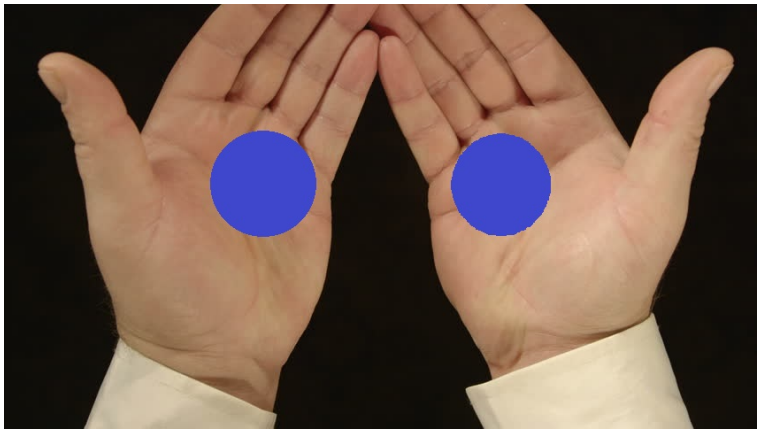
Daltonismo

- Una persona con daltonismo creerá que las esferas son del mismo color.
- ¿Cómo convencerla de que son diferentes?

Daltonismo



Daltonismo



Ali Baba

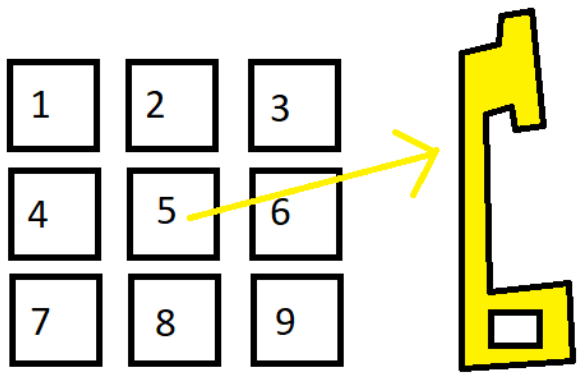
- Existe una cueva con una bifurcación, la cual es separada por una pared que puede abrirse al decir "ábrete, sésamo". Se quiere demostrar esta particularidad a otra persona, sin revelar las palabras clave ¿Es posible?

Millonario (discreto)

- Dos millonarios quieren saber si tienen la misma cantidad de dinero, pero no quieren revelar la cantidad que posee cada uno ¿Es posible?

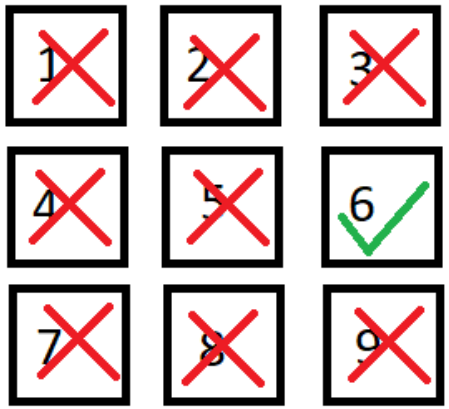
Millonario (discreto)

- Se organizan N cajas que representan las cantidades que poseen cada millonario
- Para cada acción que se realice, el otro millonario no puede estar presente
- Uno de los millonarios escoge una caja y guarda la llave que corresponde a dicha caja



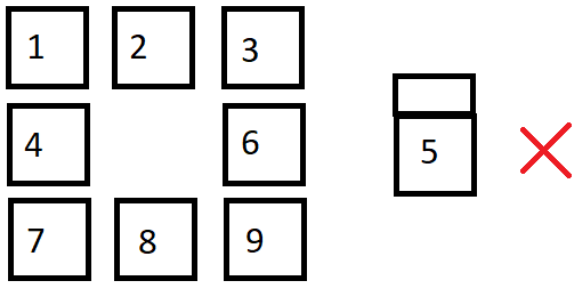
Millonario (discreto)

- El otro millonario (sin abrir las cajas) desliza una nota en cada caja. Con una nota particular, señalando cual caja representa su fortuna



Millonario (discreto)

- El primer millonario regresa y abre la caja que corresponde a su llave (no debería poder abrir otra caja)



Millonario (discreto)

- El primer millonario descarta las cajas y deja la nota en el piso
- El otro millonario entra y verifica la nota dejada en el piso
- Ambos saben si tienen la misma cantidad, desconociendo el valor del otro (el único caso donde conocerían el valor, es en el caso de que las cantidades sean iguales)

¿Para qué usarlo?

- En la criptografía actual, la mayor vulnerabilidad es el intercambio de llaves
- Si quiero ingresar a mi cuenta, debo proporcionar mi contraseña, la cual debe ser enviada (y posiblemente interceptada) por un tercero

¿Cómo usarlo?

Una posible forma de uso, es a través del problema del logaritmo discreto y un servicio de autenticación:

- Al haberme registrado, he generado mi contraseña (x)

¿Cómo usarlo?

Para iniciar sesión, se ejecuta el siguiente algoritmo

- Genero un r tal que $0 < r < p$ y lo envío al servidor como g^r
- El servidor genera un bit aleatorio b ($\{0,1\}$) y me lo envía
- Envío g^{r+bx} al servidor
- El servidor verifica $g^{r+bx} \rightarrow g^{bx} \rightarrow g^x$ (en el escenario que $b \neq 0$)
- Se genera un nuevo r y se repite el proceso (un número necesario de veces)

Casos de uso

Posibles casos de uso de Zero Knowledge Proofs

- Votación virtual
- Desarme nuclear

Votación virtual

Se debe garantizar lo siguiente

- Legitimidad (solo votantes aptos)
- Verificabilidad (mi voto fue correcto y el conteo de votos es correcto)
- Privacidad (no se sabe la particularidad de los votos)
- No Coerción (No se pueden forzar los votos)

Votación virtual

¿Cómo lograrlo?

- Se escoge una función $y = f(x)$ tal que mi voto (x) se mapee a un candidato (y). Se sugieren los protocolos Sigma, que son funciones de mapeo en espacios vectoriales.
- Si quiero verificar mi voto, el servidor genera $a = f(r)$ y me lo envía
- Escojo un c aleatorio (que pertenezca al espacio vectorial) y se lo envío al servidor
- El servidor computa $d = r + cx$ y me lo envía
- Computo $f(d) \rightarrow f(r + cx) \rightarrow f(r) + f(cx) \rightarrow f(x) = y$

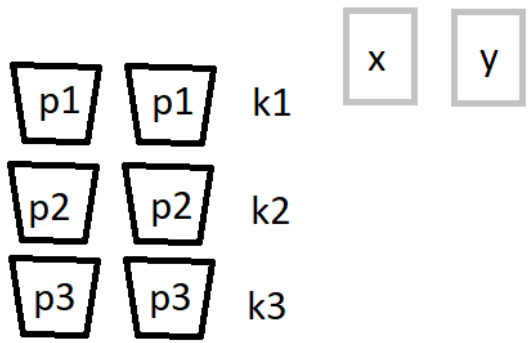
Desarme nuclear

Se debe garantizar lo siguiente

- Probar que realmente estén desarmadas las armas nucleares
- No revelar información sobre el diseño y construcción del arma nuclear

Desarme nuclear

- Se desea determinar si la cantidad canicas en dos contenedores x,y son iguales sin revelar la cantidad de canicas de dichos contenedores.



- Este problema se traslada al ámbito nuclear a través de mediciones de corrientes de neutrones (simulando las canicas).