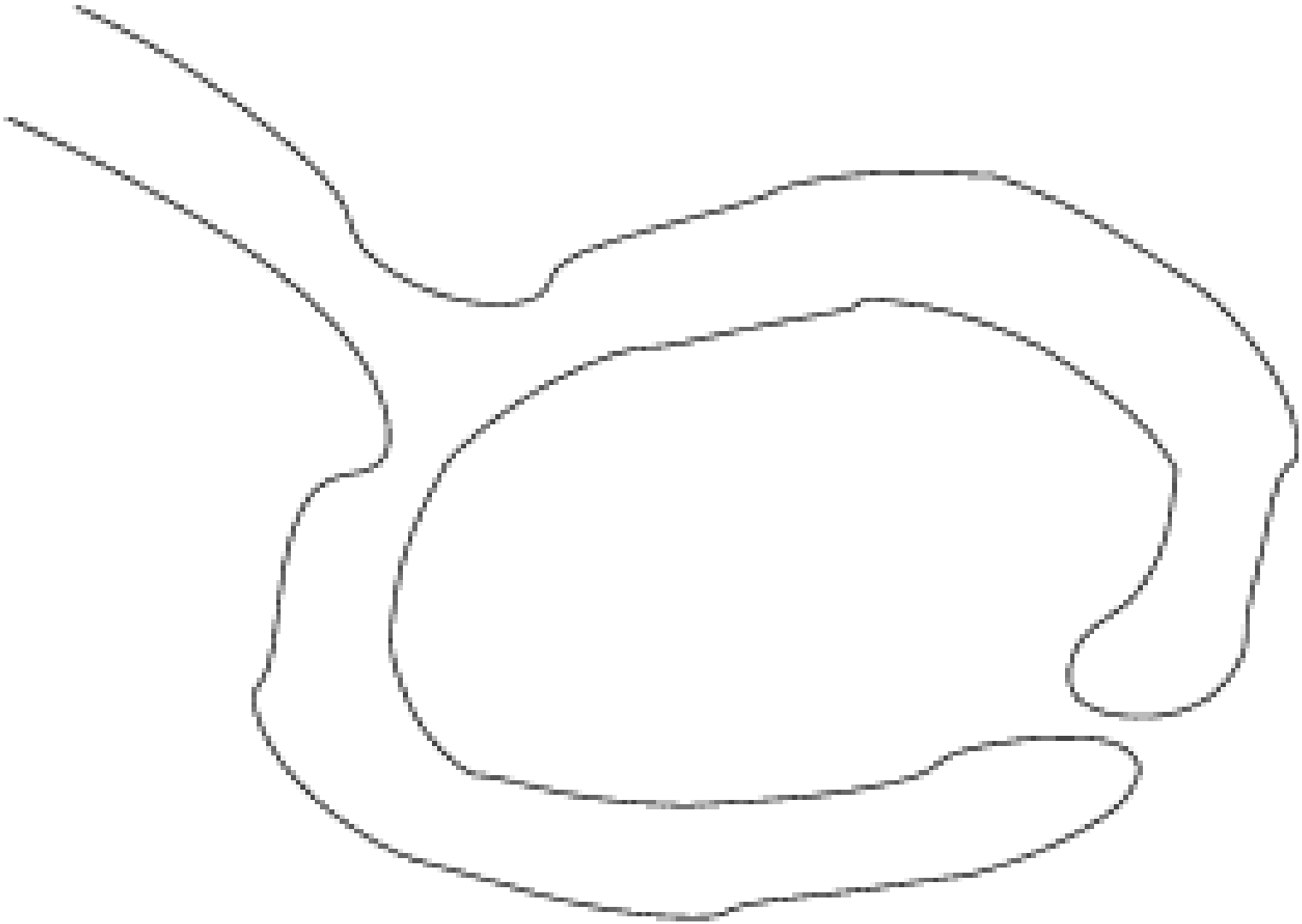
Alibaba a kúzelná jaskyňa



Stále zľahka

Máte pred sebou zadanie ťažkého sudoku.
Na papieri si ho vyriešite. Váš kamarát ho vyriešiť nevie.
Ako mu dokázať, že poznáte riešenie?
. . . ale neprezradiť nič z toho riešenia?

Challenge-response protokol

Rozložím na zadanie 81 lístočkov s číslami (face down).
Kamarát má na výber:
a) skontroluje, či tie dané v zadaní sú OK
b) vyberie blok, zamiešame lístky z neho, skontroluje 1-9

Stále zľahka

Máte pred sebou zadanie ťažkého sudoku.
Na papieri si ho vyriešite. Váš kamarát ho vyriešiť nevie.
Ako mu dokázať, že poznáte riešenie?
. . . ale neprezradiť nič z toho riešenia?

Challenge-response protokol

Rozložím na zadanie 81 lístočkov s číslami (face down).
Kamarát má na výber:
a) skontroluje, či tie dané v zadaní sú OK
b) vyberie blok, zamiešame lístky z neho, skontroluje 1-9

Serióznejší príklad

Hamiltonovská kružnica

Daný je graf G. Alenka v ňom pozná Hamiltonovskú kružnicu. Ako toto dokáže Borisovi?

Challenge-response protokol

Alenka vyrobí graf H izomorfný s G (spermutuje vrcholy).
Každú hranu H napíše na iný papierik, rozloží ich (face down).
Boris má na výber:
a) chce vidieť kružnicu: Alenka odkryje n lístočkov
b) chce vidieť všetko: Alenka odkryje všetko a povie izomorfizmus.

Serióznejší príklad

Hamiltonovská kružnica

Daný je graf G. Alenka v ňom pozná Hamiltonovskú kružnicu. Ako toto dokáže Borisovi?

Challenge-response protokol

Alenka vyrobí graf H izomorfný s G (spermutuje vrcholy).
Každú hranu H napíše na iný papierik, rozloží ich (face down).
Boris má na výber:
a) chce vidieť kružnicu: Alenka odkryje n lístočkov
b) chce vidieť všetko: Alenka odkryje všetko a povie izomorfizmus.

Seriózne zero knowledge schémy

Použitie

Autentifikácia!

1. ja poznám heslo
2. chcem o tom presvedčiť server
3. nik kto počúva sa nesmie nič dozvedieť

Bit commitment

Pri implementácii potrebujeme ekvivalent „papierika textom dole“.

Seriózne zero knowledge schémy

Použitie

Autentifikácia!

1. ja poznám heslo
2. chcem o tom presvedčiť server
3. nik kto počúva sa nesmie nič dozvedieť

Bit commitment

Pri implementácii potrebujeme ekvivalent „papierika textom dole“.