

Zero-Knowledge Protocols

Abhabongse Janthong
สถาพงศ์ จันทรทอง
Associate Visionary Architect, KBTG

Zero-Knowledge Protocols

**HOW TO ACHIEVE A
COMMUNICATION
GOAL WITHOUT
LEAKING JUST
ANYTHING?**

Abhabongse Janthong

สถาพงศ์ จันทรทอง

Associate Visionary Architect, KBTG

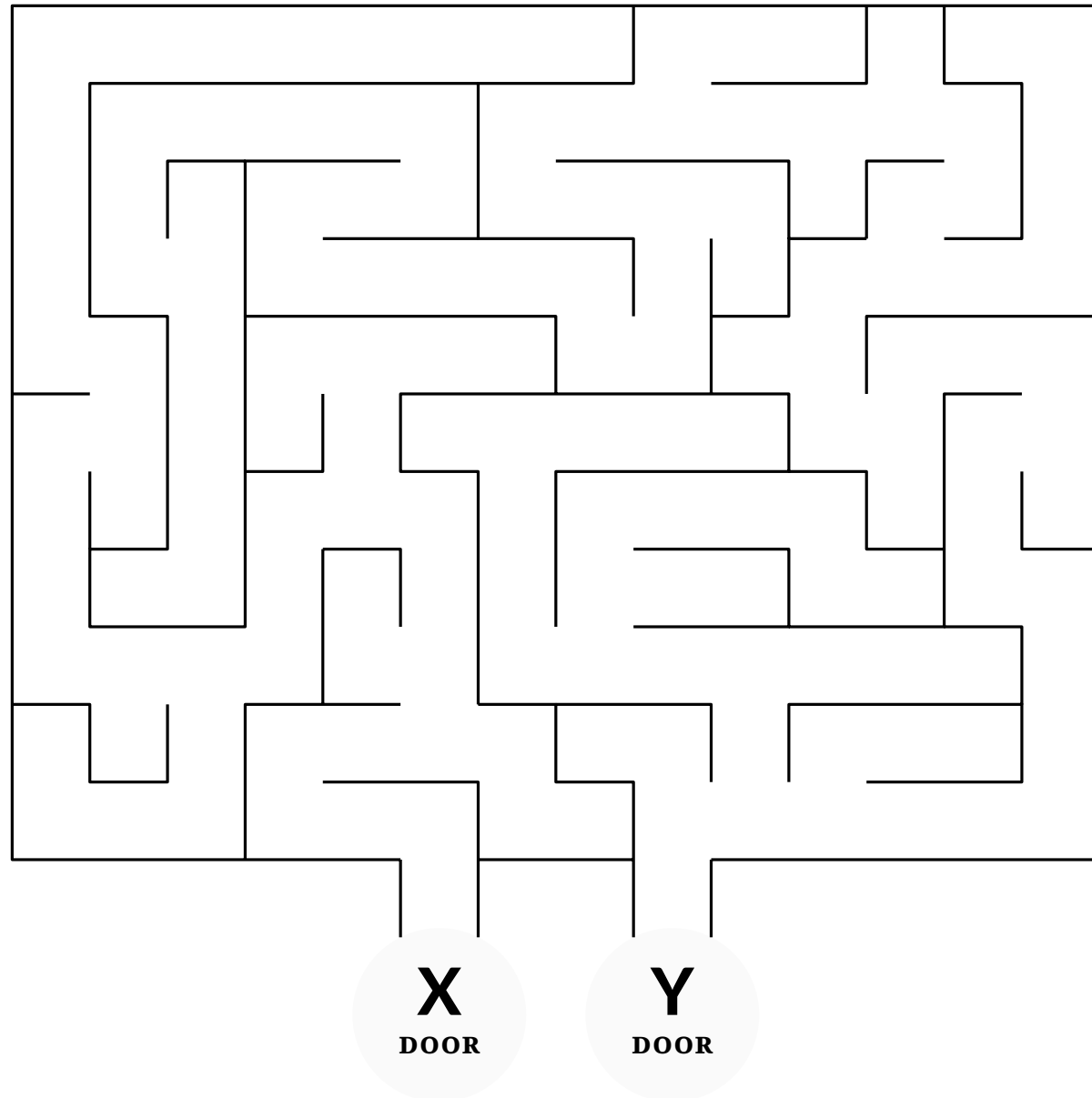
Zero-Knowledge Protocols

ต้องการสื่อสารเพื่อบรรลุ
เป้าหมายบางอย่างโดยไม่
เปิดเผยอะไรนอก
เหนือจากที่จำเป็น

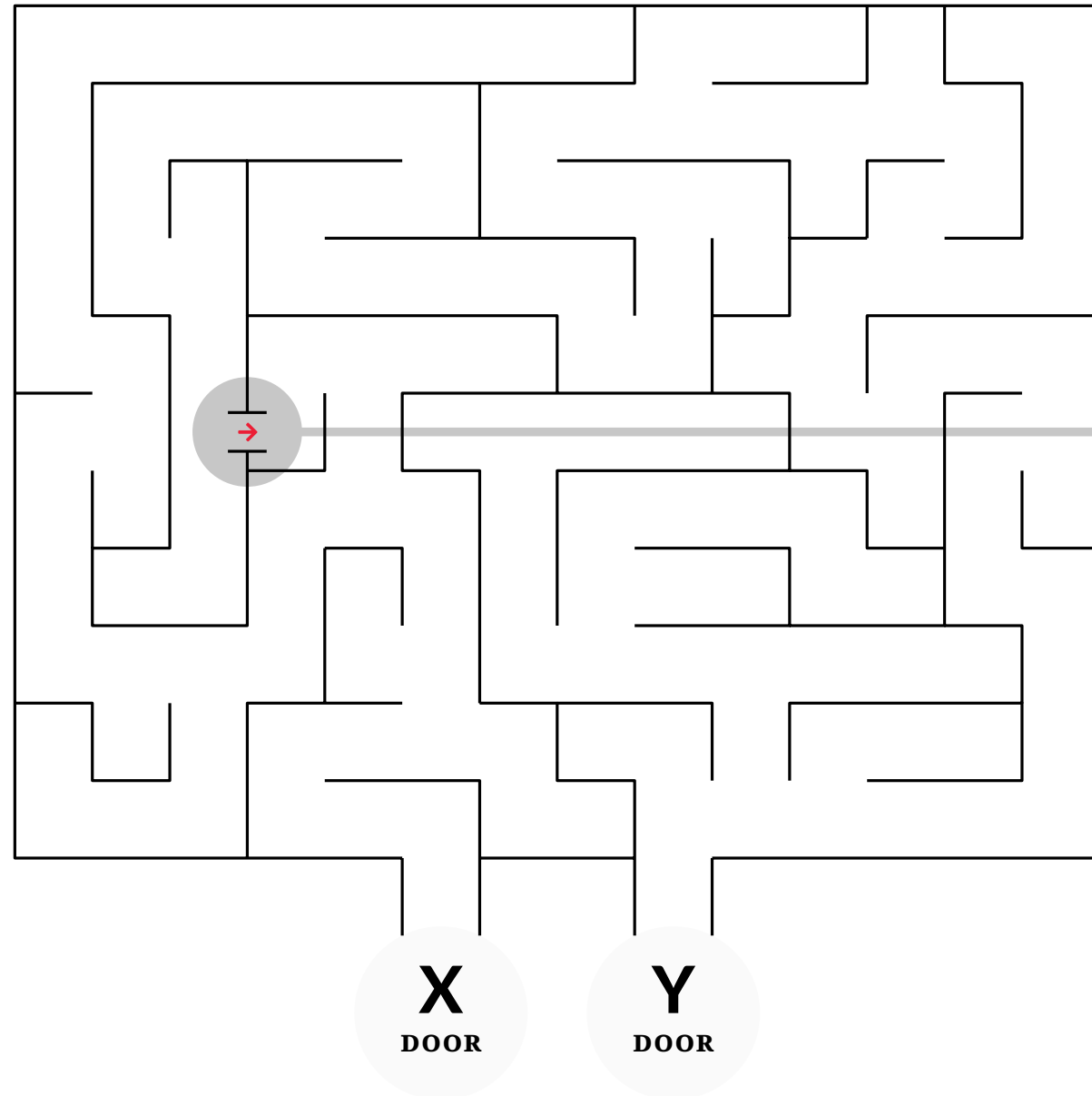
Abhabongse Janthong
อาภาพงศ์ จันทรทอง
Associate Visionary Architect, KBTG

Maze | เขาวงกต

เขาวงกตมีทางเข้า-ออก 2 ทาง และมีเส้นทางภายในที่เชื่อมด้วยกลไกปริศนาอย่างหนึ่ง



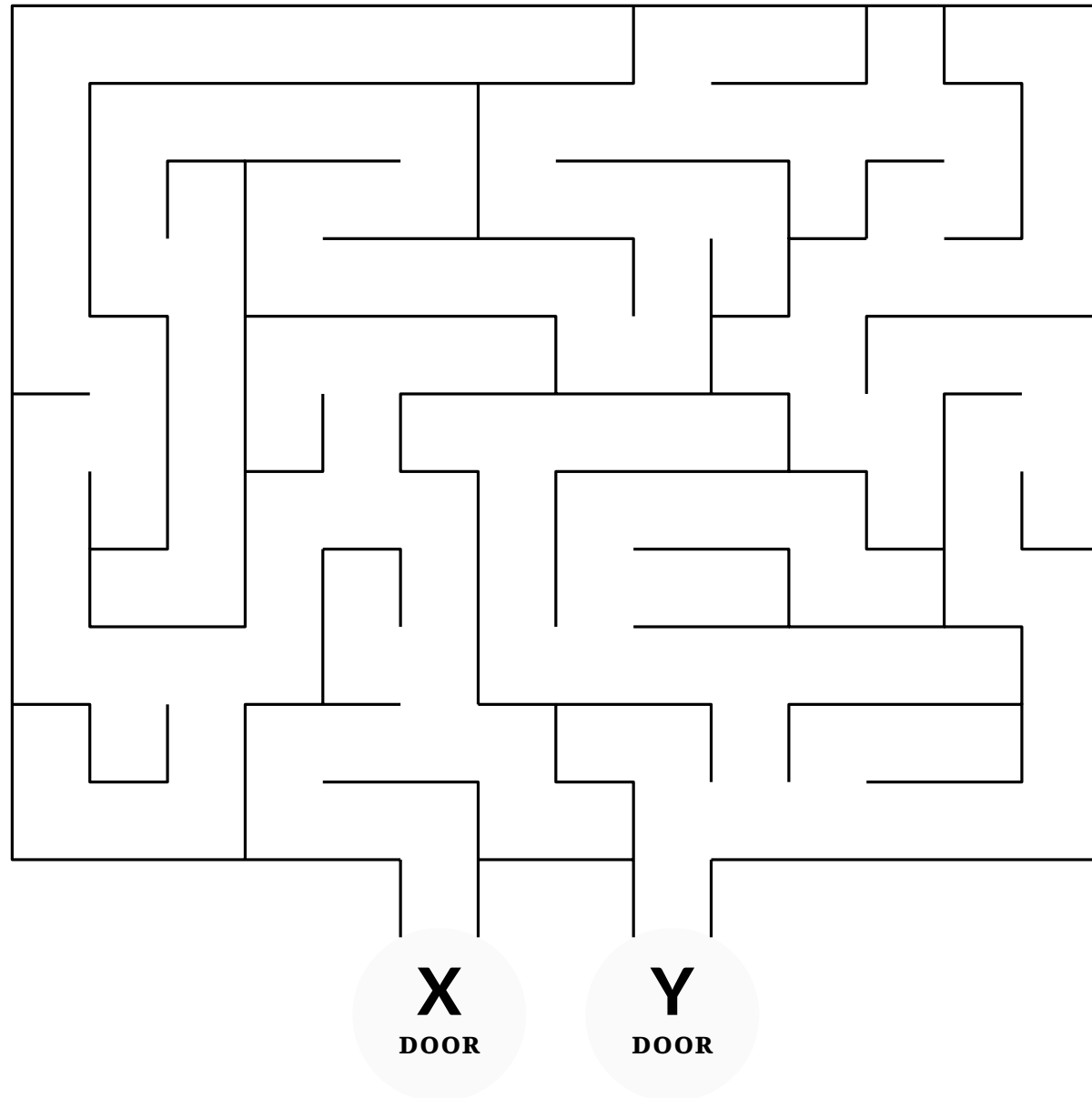
Maze | เขาวงกต



เขาวงกตมีทางเข้า-ออก 2 ทาง และมีเส้นทางภายในที่เชื่อมด้วยกลไกปริศนาอย่างหนึ่ง

(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

Maze | เขาวงกต



เขาวงกตมีทางเข้า-ออก 2 ทาง และมีเส้นทางภายในที่เชื่อมด้วยกลไกปริศนาอย่างหนึ่ง

(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

Maze | เขาวงกต



เขาวงกตมีทางเข้า-ออก 2 ทาง และมีเส้นทางภายในที่เชื่อมด้วยกลไกปริศนาอย่างหนึ่ง

(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

เราไม่เชื่อแกหรอก!!!

Maze | เขาวงกต



เขาวงกตมีทางเข้า-ออก 2 ทาง และมีเส้นทางภายในที่เชื่อมด้วยกลไกปริศนาอย่างหนึ่ง

(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

เราไม่เชื่อแกหรอก!!!

มา! เดี่ยวฉันนำทางเธอเอง

Maze | เขาวงกต



Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

เราไม่เชื่อแกหรอก!!!

มา! เดี่ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ --

Maze | เขาวงกต



Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

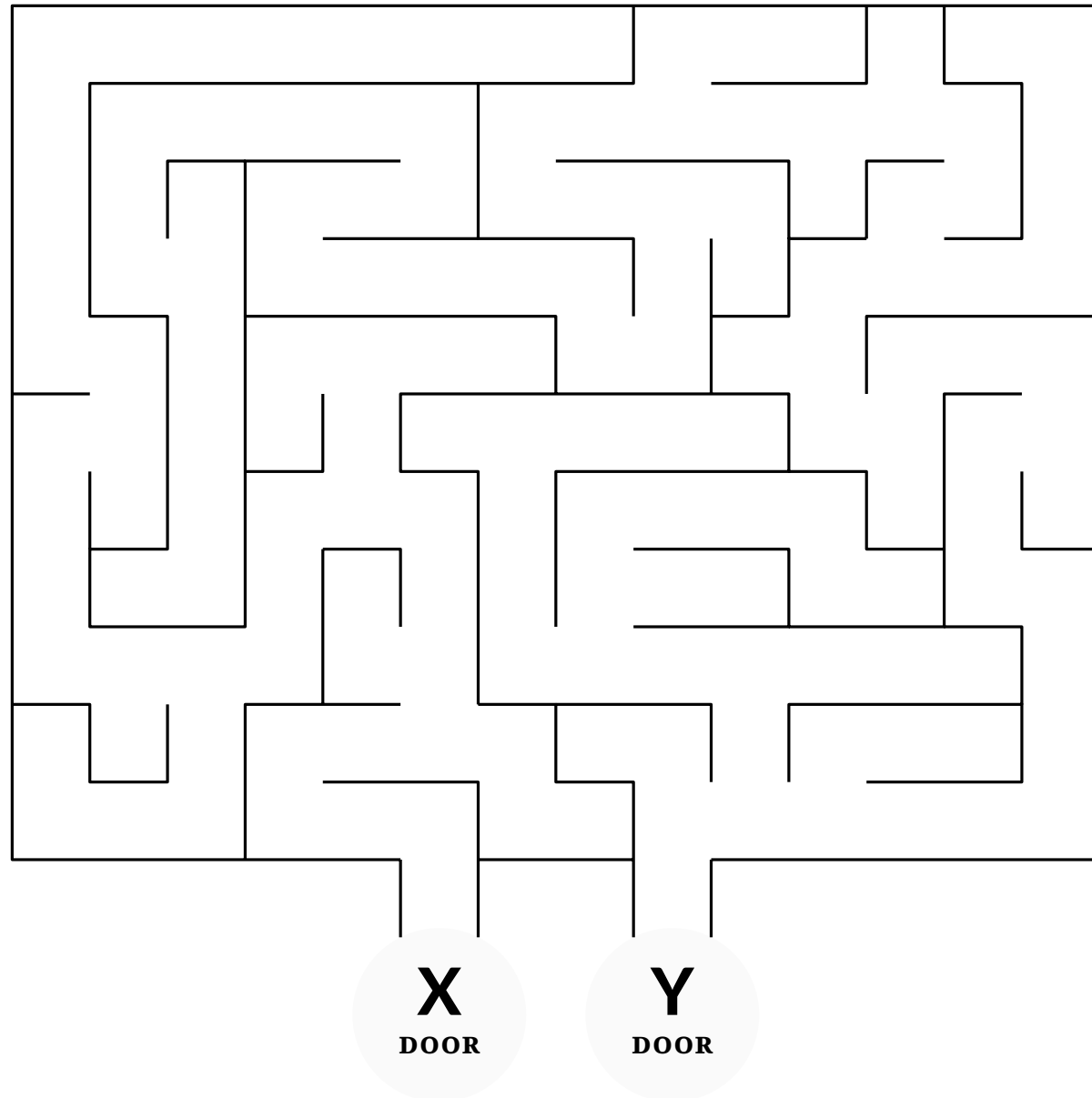
เราไม่เชื่อแกหรอก!!!

มา! เดี่ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ --

เธอนี้เรื่องมากจังนะ :(จะเอาไง

Maze | เขาวงกต



Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

เราไม่เชื่อแกหรอก!!!

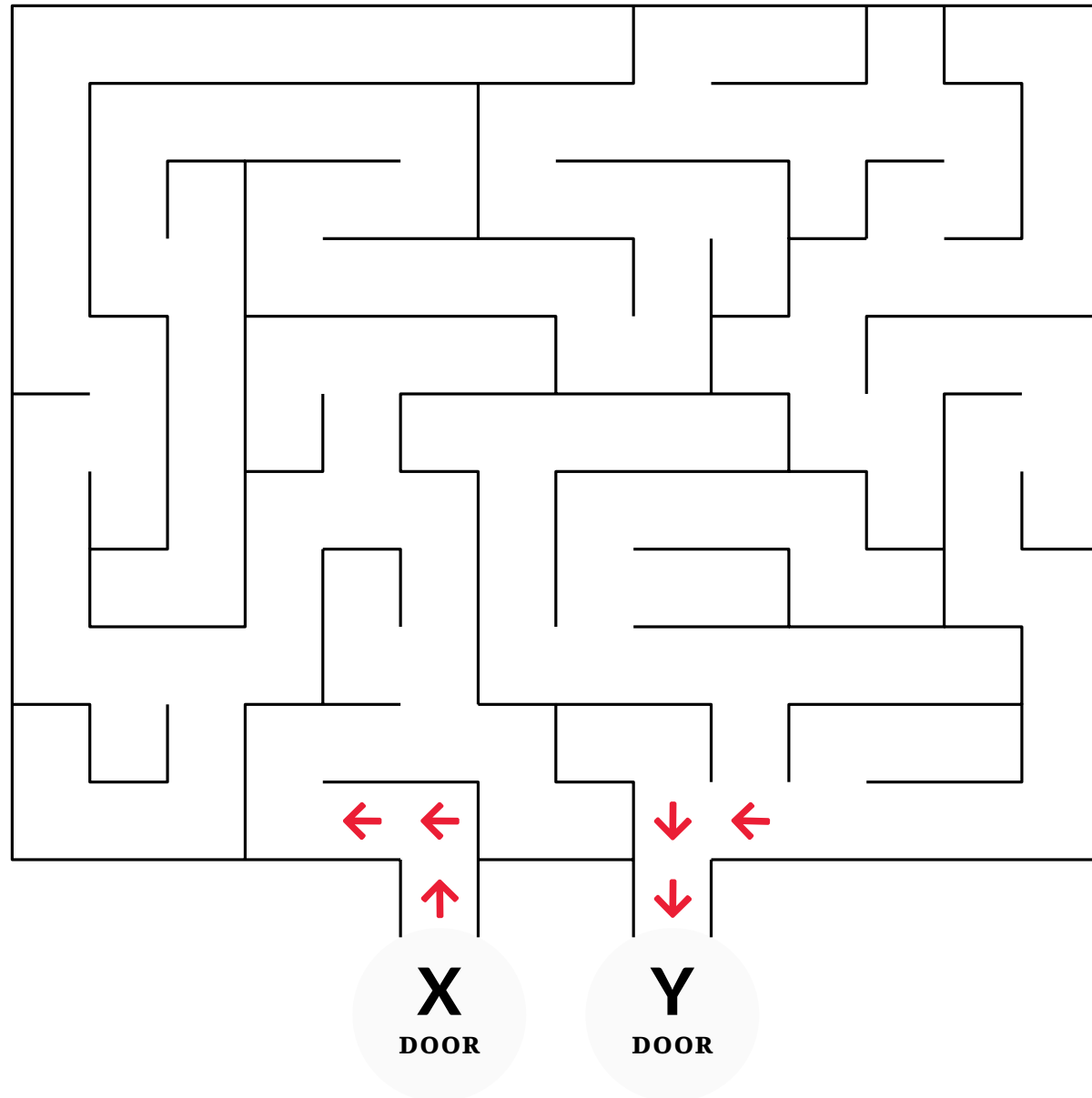
มา! เดี่ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ --

เธอนี้เรื่องมากจังนะ :(จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

Maze | เขาวงกต



ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

เราไม่เชื่อแกหรอก!!!

มา! เดี่ยวฉันนำทางเธอเอง

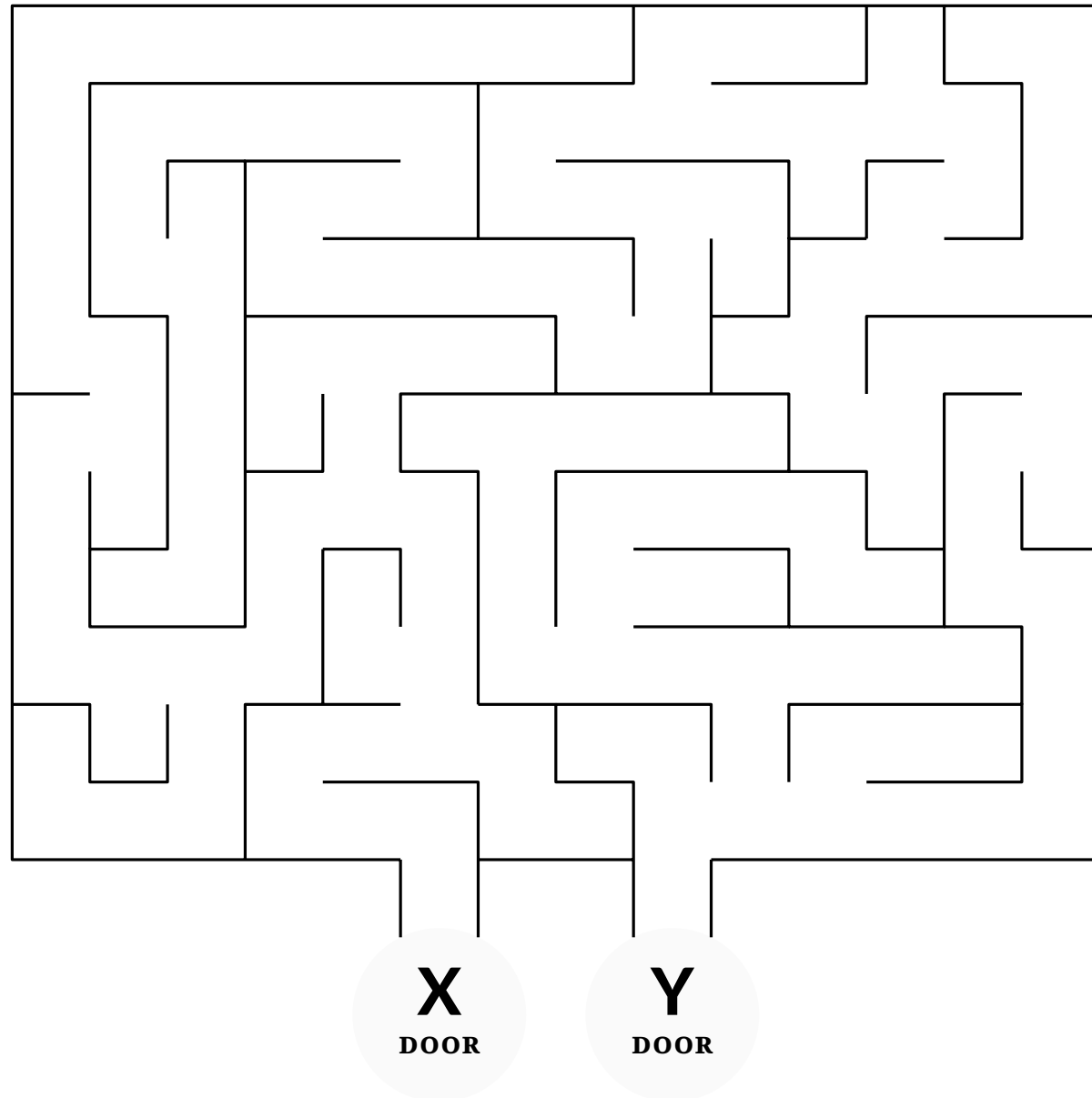
ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ --

เธอนี้เรื่องมากจังนะ :(จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

แกก็เข้าประตู **X** ไป แล้วออกทางประตู **Y** ให้เราเห็น
เดี๋ยวเราเฝ้าดูจากข้างนอกนี่แหละ

Maze | เขาวงกต



เราไม่เชื่อแกหรอก!!!

มา! เดี่ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ --

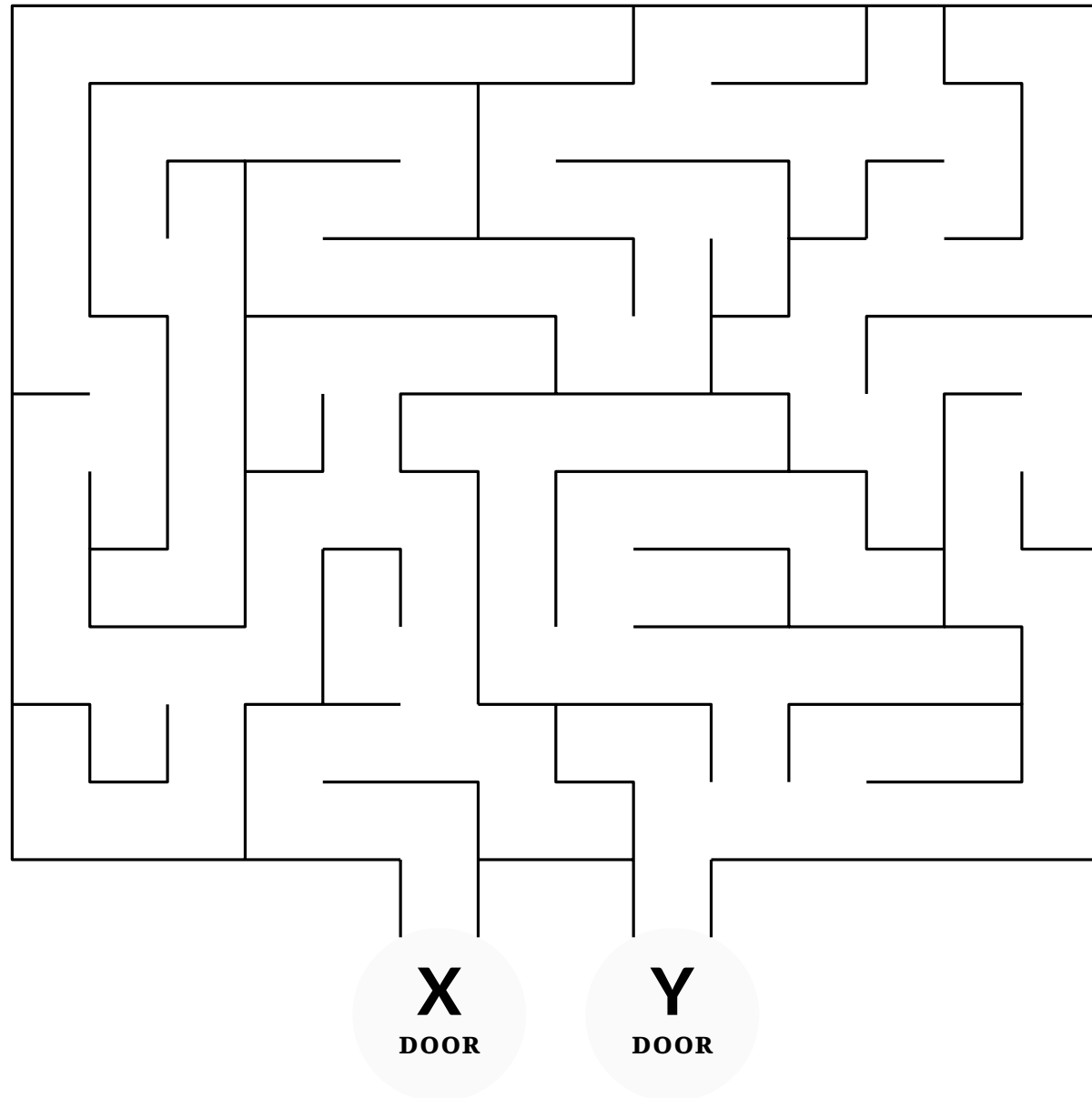
เธอนี้เรื่องมากจังนะ :(จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

แกก็เข้าประตู **X** ไป แล้วออกทางประตู **Y** ให้เราเห็น
เดี๋ยวเราเฝ้าดูจากข้างนอกนี่แหละ

ถ้าแบบนั้น ก็เท่ากับให้คำใบ้นะสิ

Maze | เขาวงกต



มา! เดี่ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ --

เธอนี้เรื่องมากจังนะ :(จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

แกก็เข้าประตู **X** ไป แล้วออกทางประตู **Y** ให้เราเห็น
เดี๋ยวเราเฝ้าดูจากข้างนอกนี่แหละ

ถ้าแบบนั้น ก็เท่ากับให้คำใบ้หะสิ

... ว่ามีทางเข้า-ออกเขาวงกต ที่ต้องเข้าจาก
ประตู **X** แล้วออกทางประตู **Y**

Maze | เขาวงกต



ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ --

เธอนี้เรื่องมากจังนะ :(จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

แกก็เข้าประตู **X** ไป แล้วออกทางประตู **Y** ให้เราเห็น
เดี๋ยวเราเฝ้าดูจากข้างนอกนี่แหละ

ถ้าแบบนั้น ก็เท่ากับให้คำใบ้นะสิ

... ว่ามีทางเข้า-ออกเขาวงกต ที่ต้องเข้าจาก
ประตู **X** แล้วออกทางประตู **Y**

เธอไม่ควรรู้ด้วยซ้ำว่ามีเส้นทางแบบนั้น
มันก็คือสปอยล์รูปแบบหนึ่งนะ

Zero – Knowledge Proof

Zero-Knowledge Proof

เป้าหมายการสื่อสาร พิสูจน์ข้อเท็จจริงบางอย่างให้อีกฝ่ายทราบ

Zero – Knowledge Proof

เป้าหมายการสื่อสาร

พิสูจน์ข้อเท็จจริงบางอย่างให้อีกฝ่ายทราบ

เงื่อนไข

ผู้ฟังต้องไม่เรียนรู้สิ่งอื่นใดเพิ่มเติมว่าทำไมข้อเท็จจริงถึงถูกต้อง

Zero – Knowledge Proof

เป้าหมายการสื่อสาร พิสูจน์ข้อเท็จจริงบางอย่างให้อีกฝ่ายทราบ

เงื่อนไข ผู้ฟังต้องไม่เรียนรู้สิ่งอื่นใดเพิ่มเติมว่าทำไมข้อเท็จจริงถึงถูกต้อง

เช่น พิสูจน์ว่า บางปัญหามีคำตอบ แต่ ไม่บอกคำตอบ ✓

Zero – Knowledge Proof

เป้าหมายการสื่อสาร พิสูจน์ข้อเท็จจริงบางอย่างให้อีกฝ่ายทราบ

เงื่อนไข ผู้ฟังต้องไม่เรียนรู้สิ่งอื่นใดเพิ่มเติมว่าทำไมข้อเท็จจริงถึงถูกต้อง

เช่น พิสูจน์ว่า บางปัญหามีคำตอบ แต่ ไม่บอกคำตอบ ✓

 พิสูจน์ว่า ฉันอายุ 18 ปีขึ้นไป แต่ ไม่บอกวันเดือนปีเกิด 📅

Zero – Knowledge Proof

เป้าหมายการสื่อสาร พิสูจน์ข้อเท็จจริงบางอย่างให้อีกฝ่ายทราบ

เงื่อนไข ผู้ฟังต้องไม่เรียนรู้สิ่งอื่นใดเพิ่มเติมว่าทำไมข้อเท็จจริงถึงถูกต้อง

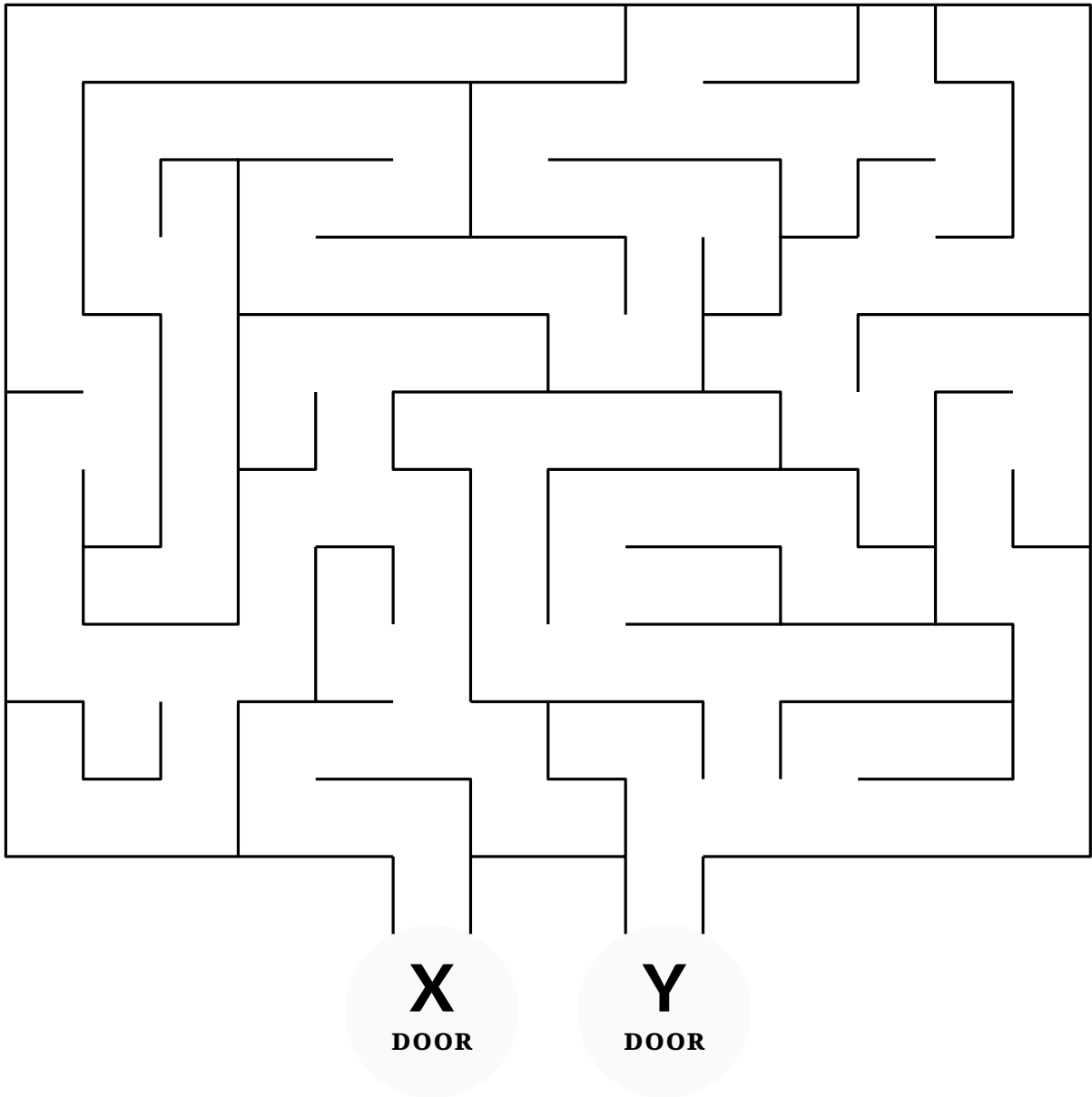
เช่น พิสูจน์ว่า บางปัญหามีคำตอบ แต่ ไม่บอกคำตอบ ✓

พิสูจน์ว่า ฉันอายุ 18 ปีขึ้นไป แต่ ไม่บอกวันเดือนปีเกิด 📅

พิสูจน์ว่า ฉันมีสิทธิเข้าถึงข้อมูล แต่ ไม่บอก credentials / secret key 🔑

~~พิสูจน์ว่า บางปัญหาแก้ไขได้ แต่ ไม่บอกวิธีแก้ไข~~ 😞

Solving Maze | หาทางออก



Alice ผู้พิสูจน์

ผู้ตรวจสอบ Bob

Solving Maze | หาทางออก



Alice ผู้พิสูจน์

ผู้ตรวจสอบ **Bob**

เอาอย่างนี้แล้วกัน (1) เดินเธอหันหลังก่อน
แล้วฉันจะเดินเข้าไปเตรียมตัวข้างใน จากนั้น
(2) เดินฉันจะเดินออกมาให้เธอดู

Solving Maze | หาทางออก



Alice ผู้พิสูจน์

ผู้ตรวจสอบ **Bob**

เอาอย่างนี้แล้วกัน (1) เดี๋ยวเธอหันหลังก่อน
แล้วฉันจะเดินเข้าไปเตรียมตัวข้างใน จากนั้น
(2) เดี๋ยวฉันจะเดินออกมาให้เธอดู

ทำแบบนี้แล้วเธอก็ไม่รู้ว่าฉันเดินเข้าประตูไหน

Solving Maze | หาทางออก



Alice ผู้พิสูจน์

ผู้ตรวจสอบ **Bob**

เอาอย่างนี้แล้วกัน (1) เดินเธอหันหลังก่อน
แล้วฉันจะเดินเข้าไปเตรียมตัวข้างใน จากนั้น
(2) เดินฉันจะเดินออกมาให้เธอดู

ทำแบบนี้แล้วเธอก็ไม่รู้ว่าฉันเดินเข้าประตูไหน

อ้าว! แล้วแบบนี้จะรู้ได้ไงว่าแกไม่ได้กลับ
ออกมาทางเดิมที่แกเดินเข้าไป

Solving Maze | หาทางออก



Alice ผู้พิสูจน์

ผู้ตรวจสอบ **Bob**

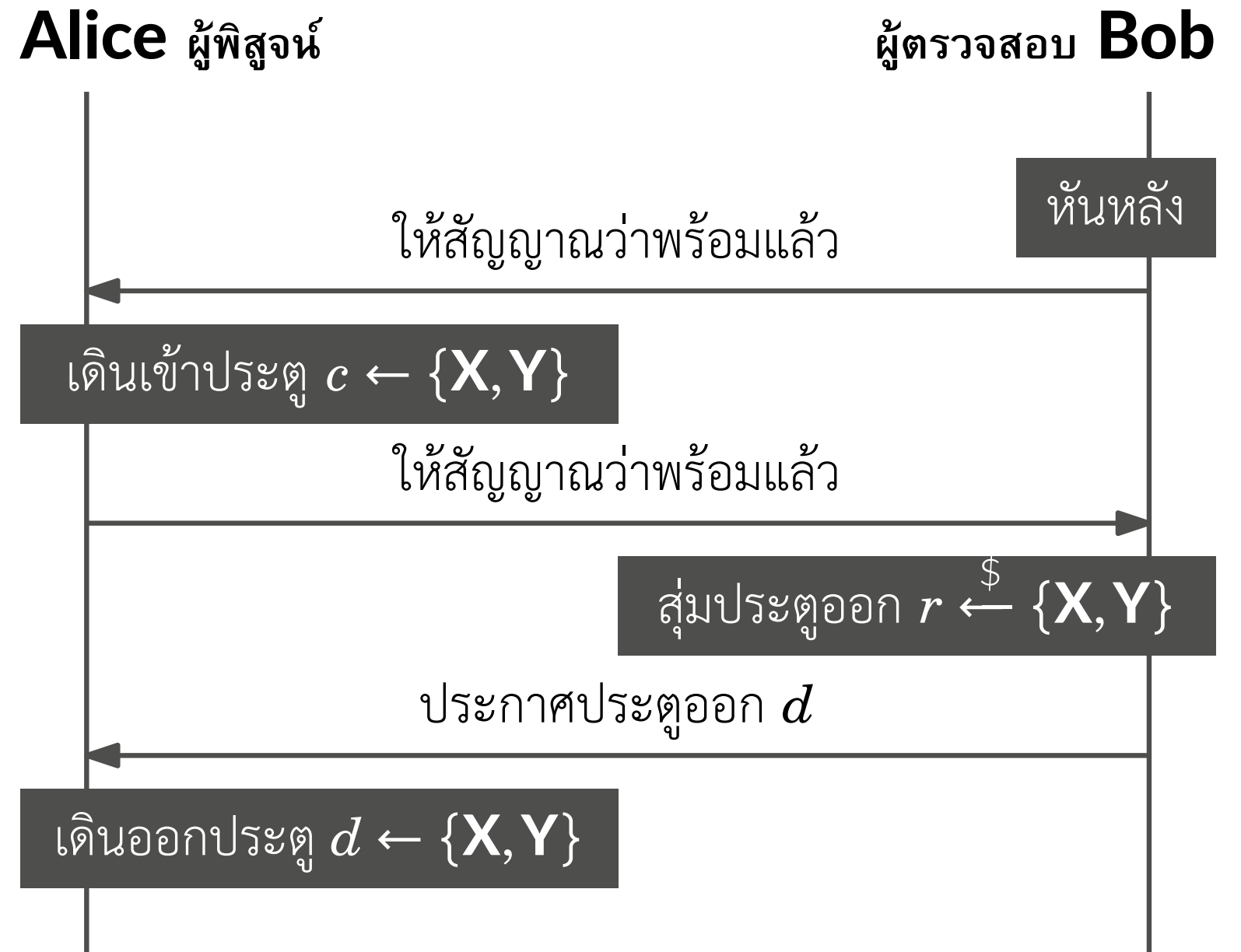
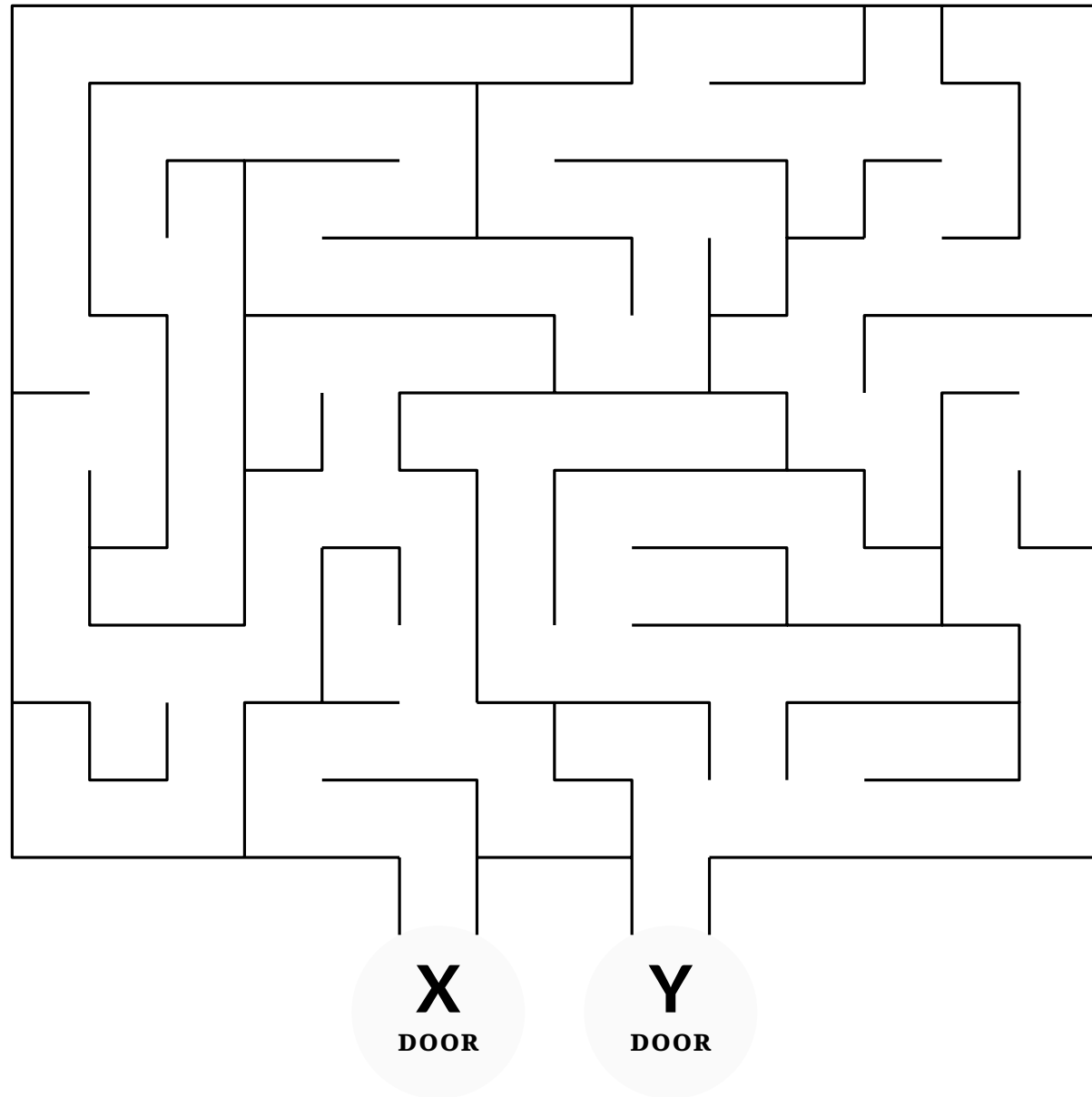
เอาอย่างนี้แล้วกัน (1) เดินเธอหันหลังก่อน
แล้วฉันจะเดินเข้าไปเตรียมตัวข้างใน จากนั้น
(2) เดินฉันจะเดินออกมาให้เธอดู

ทำแบบนี้แล้วเธอก็ไม่รู้ว่าฉันเดินเข้าประตูไหน

อ้าว! แล้วแบบนี้จะรู้ได้ไงว่าแกไม่ได้กลับ
ออกมาทางเดิมที่แกเดินเข้าไป

เธอก็สุ่มสิว่าจะให้ฉันเดินออกทางประตูไหน
ถ้าฉันรู้วิธีแก้เขาวงกต ฉันจะเดินออกประตู
ไหนก็ได้ / แต่ถ้าฉันไม่รู้ ฉันต้องเดาใจเธอไง

Solving Maze | หาทางออก



THE HEART OF Zero-Knowledge Proof

THE HEART OF Zero-Knowledge Proof

COMPLETENESS

ถ้า **Alice** ทราบคำตอบจริง

แล้ว **Alice** สามารถพิสูจน์
ข้อเท็จจริงให้ **Bob** กระทำได้

THE HEART OF Zero-Knowledge Proof

COMPLETENESS

ถ้า **Alice** ทราบคำตอบจริง

แล้ว **Alice** สามารถพิสูจน์
ข้อเท็จจริงให้ **Bob** กระทำได้

SOUNDNESS

ถ้า **Alice** ไม่ทราบคำตอบ

แล้ว **Alice** ไม่สามารถหลอก
ให้ **Bob** เชื่อคล้อยตามได้

THE HEART OF Zero-Knowledge Proof

COMPLETENESS

ถ้า **Alice** ทราบคำตอบจริง

แล้ว **Alice** สามารถพิสูจน์
ข้อเท็จจริงให้ **Bob** กระจ่างได้

SOUNDNESS

ถ้า **Alice** ไม่ทราบคำตอบ

แล้ว **Alice** ไม่สามารถหลอก
ให้ **Bob** เชื่อคล้อยตามได้

ZERO-KNOWLEDGE

ถ้า **Alice** ทราบคำตอบจริง

แล้ว **Bob** ไม่ได้เรียนรู้สิ่งใด
จาก **Alice** เว้นเฉพาะสิ่งที่
Bob คาดเดาได้ด้วยตนเอง

THE HEART OF Zero-Knowledge Proof

COMPLETENESS

ถ้า **Alice** ทราบคำตอบจริง

แล้ว **Alice** สามารถพิสูจน์
ข้อเท็จจริงให้ **Bob** กระจ่างได้

**ด้วยความน่าจะเป็นที่สูงมาก ๆ*

SOUNDNESS

ถ้า **Alice** ไม่ทราบคำตอบ

แล้ว **Alice** ไม่สามารถหลอก
ให้ **Bob** เชื่อคล้อยตามได้

**ด้วยความน่าจะเป็นที่สูงมาก ๆ*

ZERO-KNOWLEDGE

ถ้า **Alice** ทราบคำตอบจริง

แล้ว **Bob** ไม่ได้เรียนรู้สิ่งใด
จาก **Alice** เว้นเฉพาะสิ่งที่
Bob คาดเดาได้ด้วยตนเอง

**ด้วยความน่าจะเป็นที่สูงมาก ๆ*

CORRECTNESS PROPERTY

SECURITY PROPERTY