Zero-Knowledge Protocols

Abhabongse Janthong
อาภาพงศ์ จันทร์ทอง
Associate Visionary Architect, KBTG

Zero-Knowledge Protocols

HOW TO ACHIEVE A COMMUNICATION GOAL WITHOUT LEAKING JUST ANYTHING?

Abhabongse Janthong
อาภาพงศ์ จันทร์ทอง
Associate Visionary Architect, KBTG

Zero-Knowledge Protocols

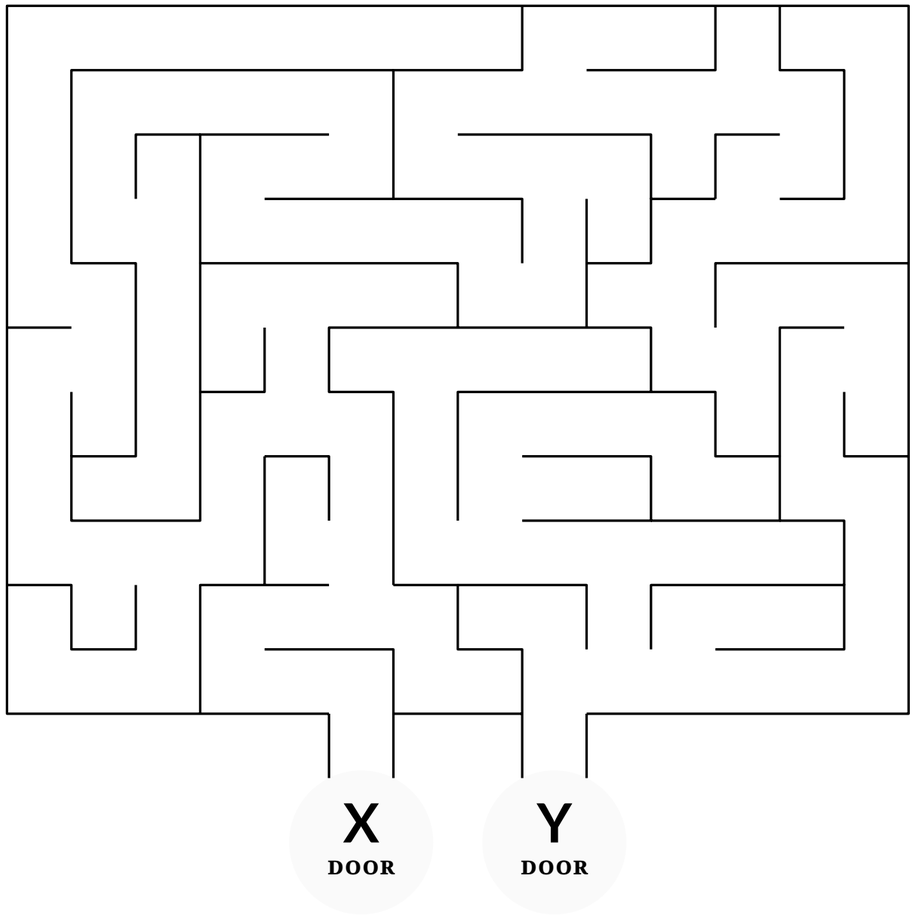
ต้องการสื่อสารเพื่อบรรลุเป้าหมายบางอย่างโดยไม่เปิดเผยอะไรนอกเหนือจากที่จำเป็น

Abhabongse Janthong
อาภาพงศ์ จันทร์ทอง
Associate Visionary Architect, KBTG

Act I

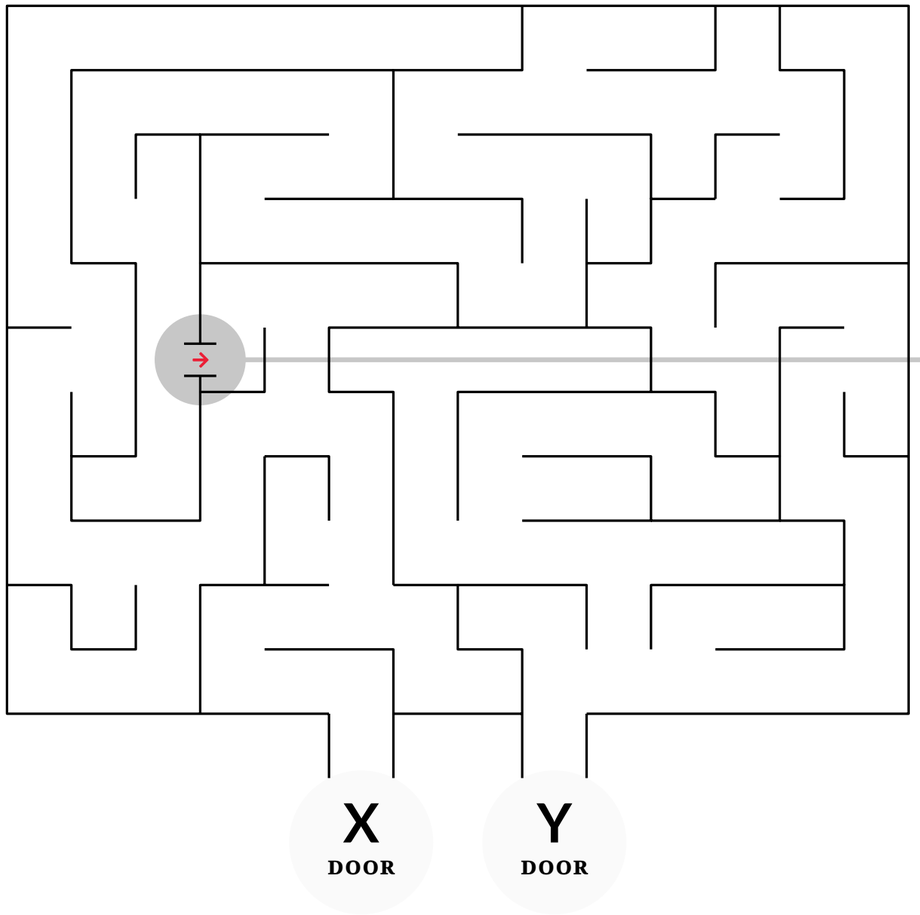
IN-DEPTH TECHNICAL DEMO

เขาวงกต ▶ โจทย์



เขาวงกตมี**ทางเข้า–ออก 2 ทาง** และมีเส้นทางภายในที่เชื่อมด้วย**กลไกปริศนา**อย่างหนึ่ง

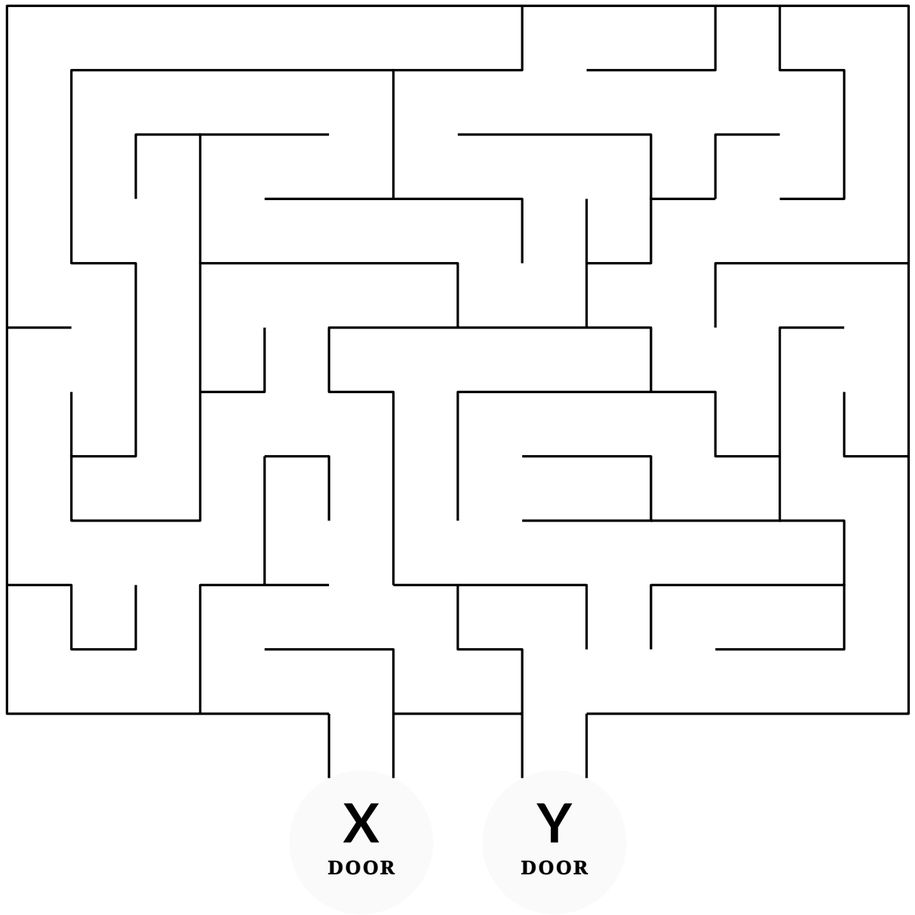
เขาวงกต ▶ โจทย์



เขาวงกตมี**ทางเข้า–ออก 2 ทาง** และมีเส้นทางภายในที่เชื่อมด้วย**กลไกปริศนา**อย่างหนึ่ง

(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

เขาวงกต ▶ โจทย์



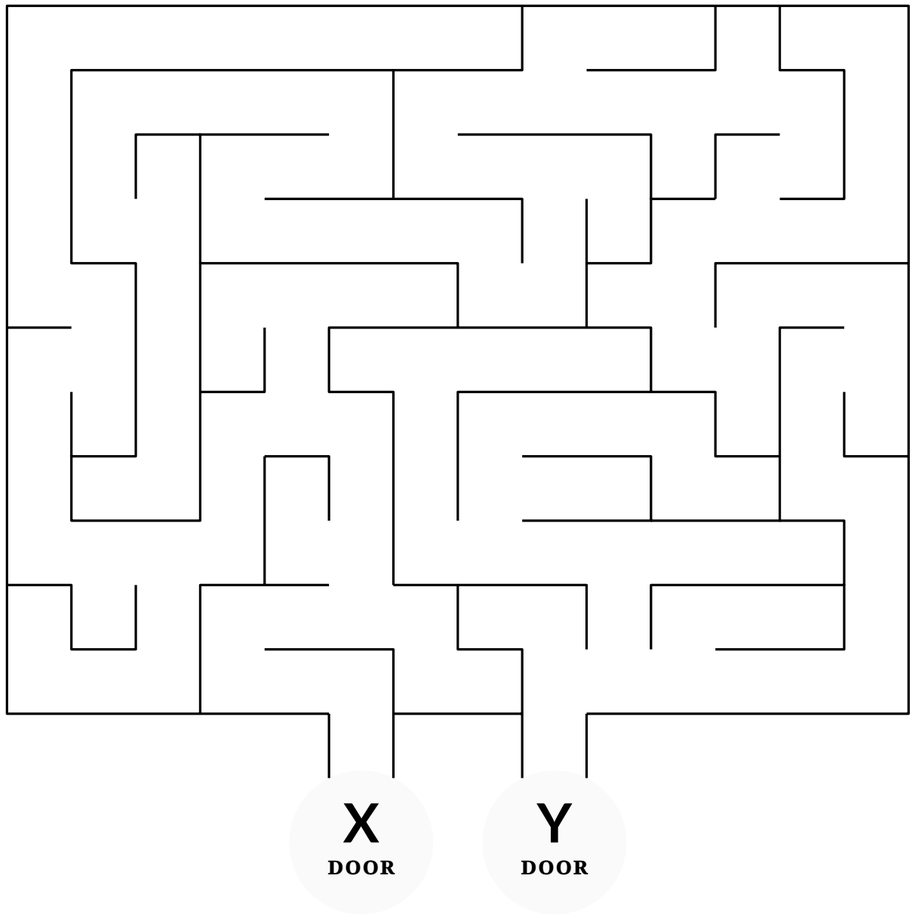
เขาวงกตมี**ทางเข้า–ออก 2 ทาง** และมีเส้นทางภายในที่เชื่อมด้วย**กลไกปริศนา**อย่างหนึ่ง

(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

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

เขาวงกต ▶ โจทย์



เขาวงกตมี**ทางเข้า–ออก 2 ทาง** และมีเส้นทางภายในที่เชื่อมด้วย**กลไกปริศนา**อย่างหนึ่ง

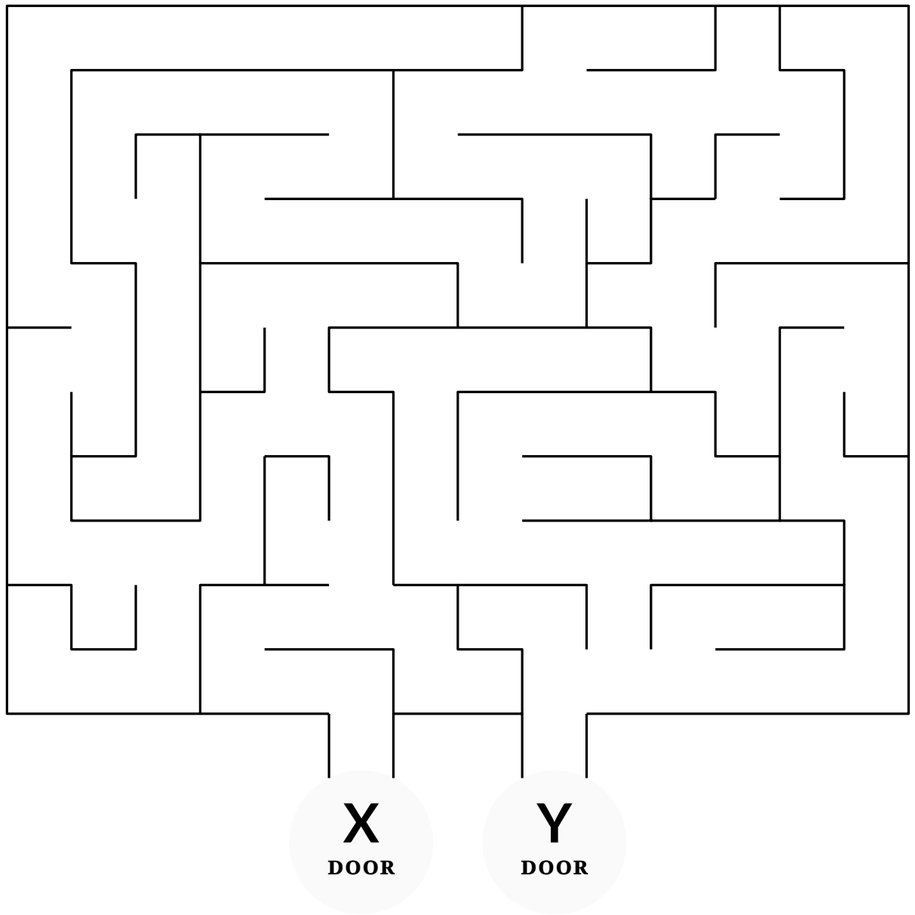
(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

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

เราไม่เชื่อแกหรอก!!!

เขาวงกต ▶ โจทย์



เขาวงกตมี**ทางเข้า–ออก 2 ทาง** และมีเส้นทางภายในที่เชื่อมด้วย**กลไกปริศนา**อย่างหนึ่ง

(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

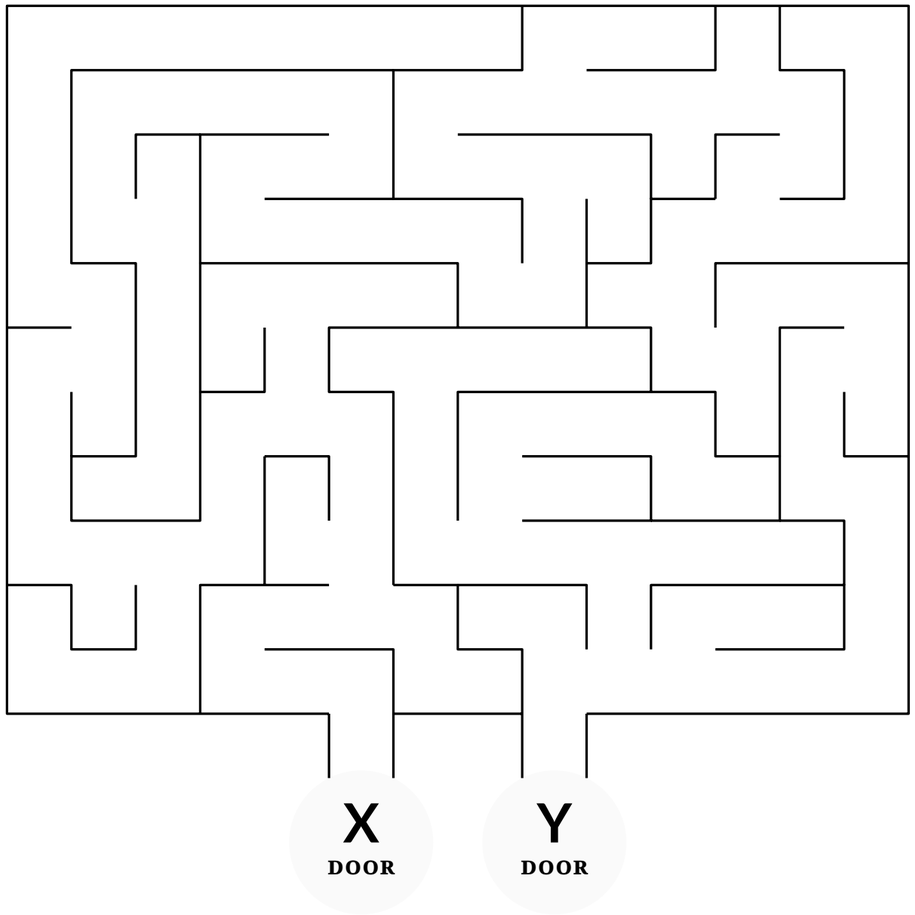
Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

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

เราไม่เชื่อแกหรอก!!!

มา! เดี๋ยวฉันนำทางเธอเอง

เขาวงกต ▶ โจทย์



Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

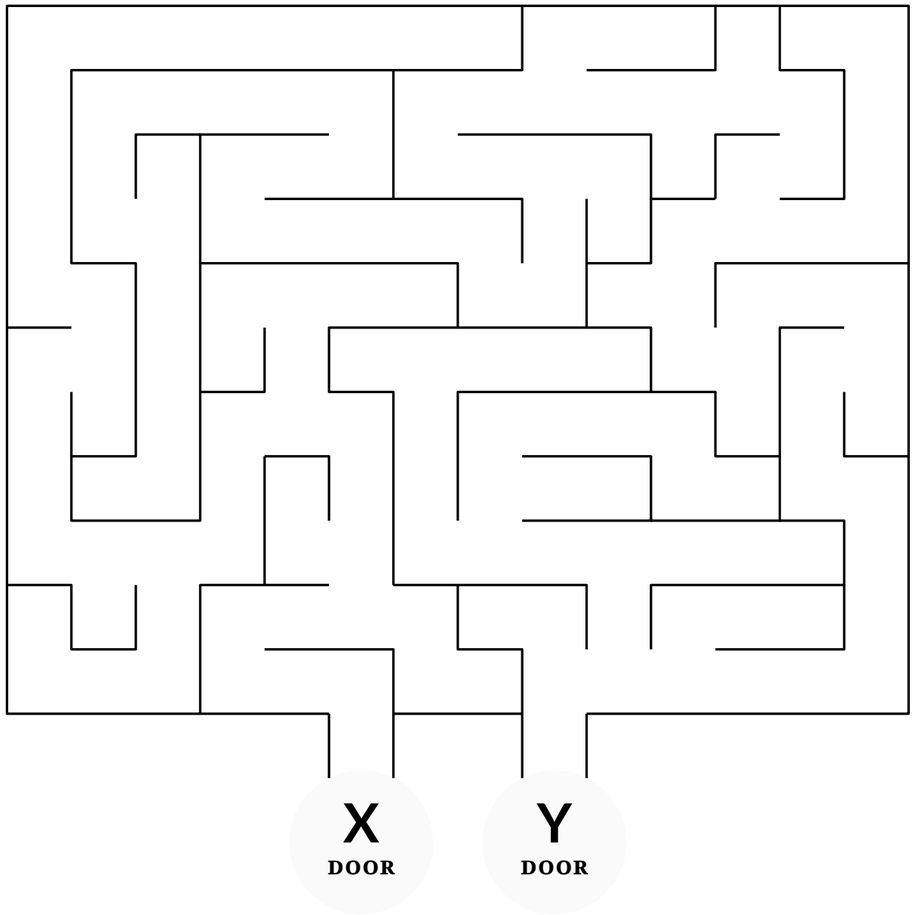
ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** *และประตู* **Y**

เราไม่เชื่อแกหรอก!!!

มา! เดี๋ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ -_-

เขาวงกต ▶ โจทย์



Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

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

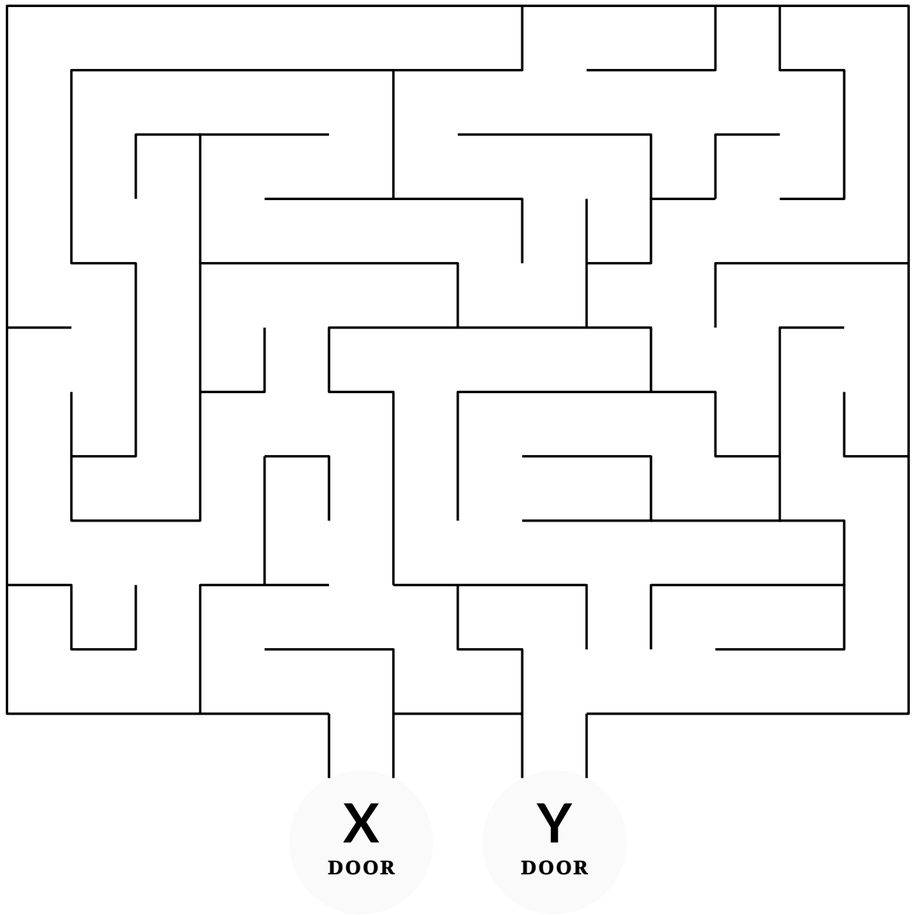
เราไม่เชื่อแกหรอก!!!

มา! เดี๋ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ -_-

เธอนี่เรื่องมากจังนะ :(จะเอาไง

เขาวงกต ▶ โจทย์



Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

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

เราไม่เชื่อแกหรอก!!!

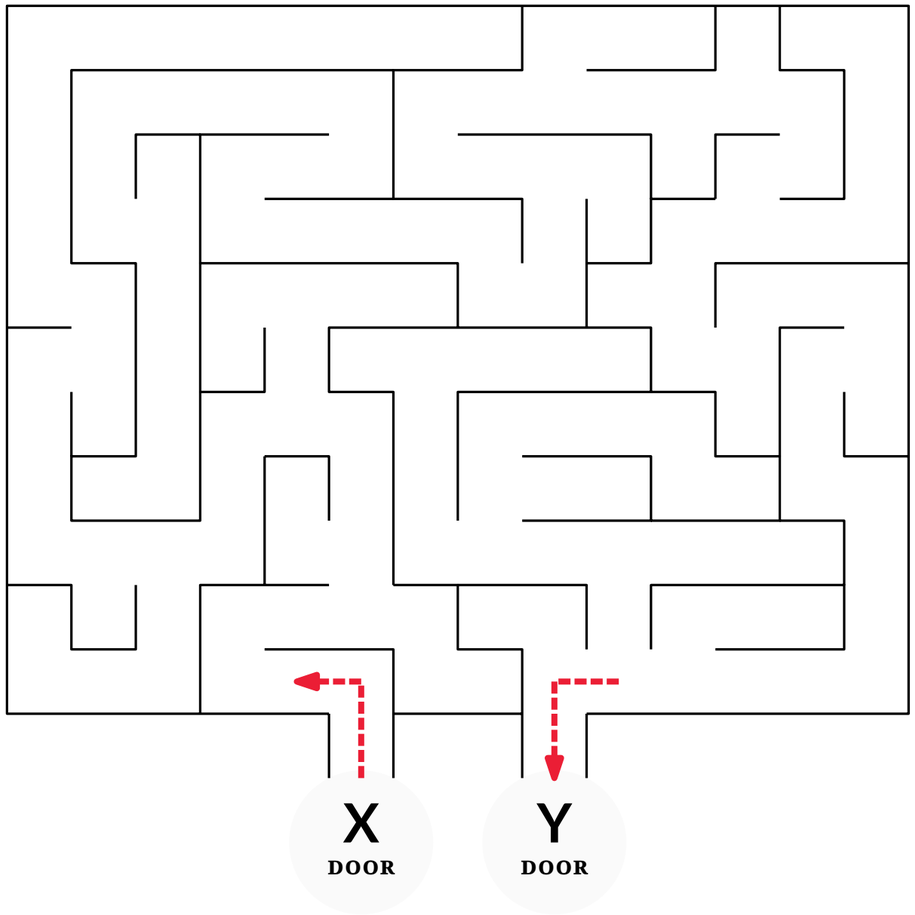
มา! เดี๋ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ -_-

เธอนี่เรื่องมากจังนะ :(จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

เขาวงกต ▶ โจทย์



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

เราไม่เชื่อแกหรอก!!!

มา! เดี๋ยวฉันนำทางเธอเอง

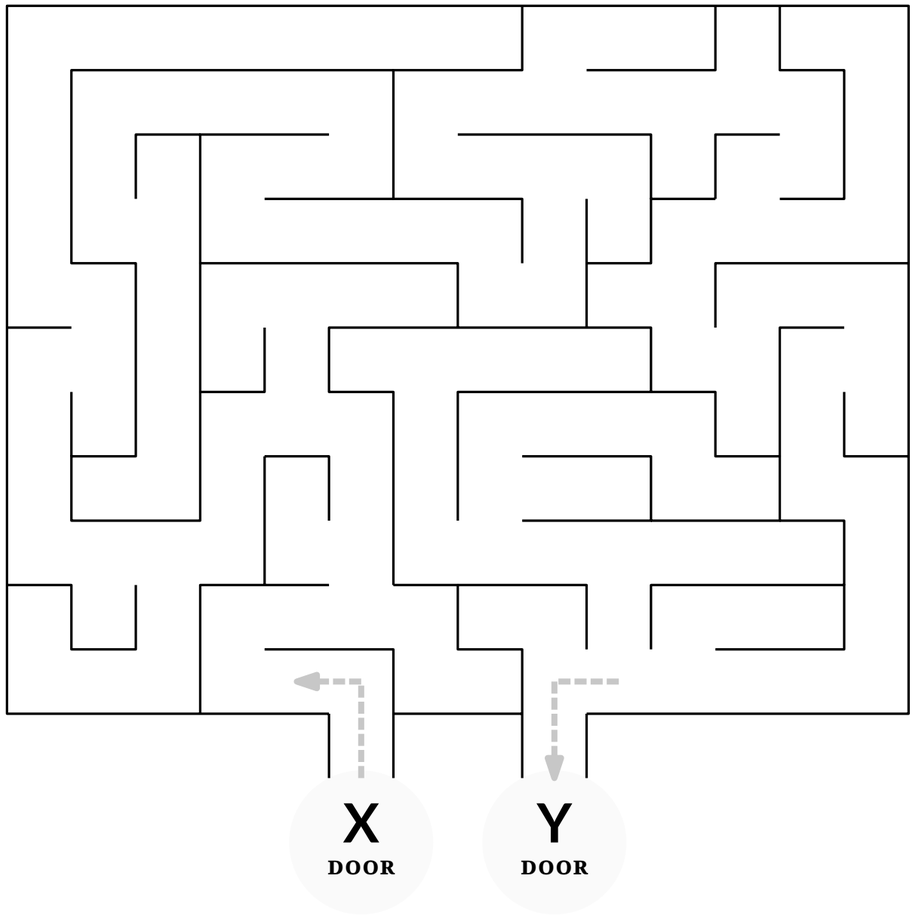
ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ -_-

เธอนี่เรื่องมากจังนะ :(จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

แกก็เข้าประตู **X** ไป แล้วออกทางประตู **Y** ให้เราเห็น
เดี๋ยวเราเฝ้าดูจากข้างนอกนี้นี่แหละ

เขาวงกต ▶ โจทย์



เราไม่เชื่อแกหรอก!!!

มา! เดี๋ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ -_-

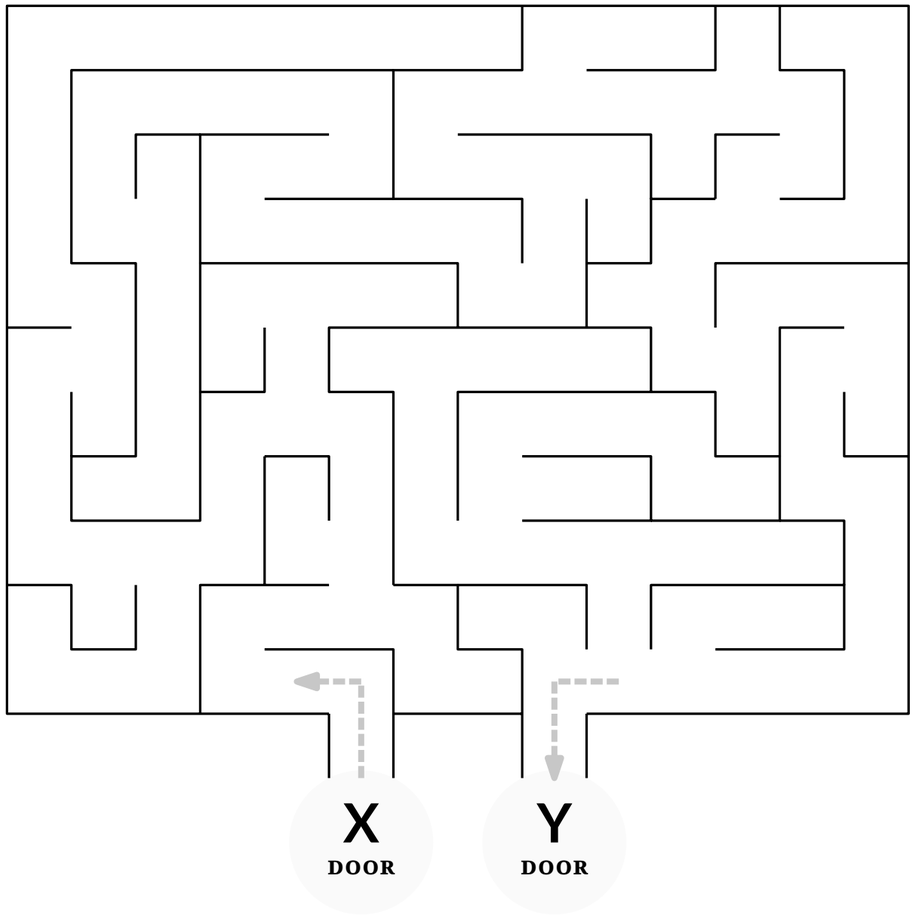
เธอนี่เรื่องมากจังนะ :(จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

*แกก็เข้าประตู **X** ไป แล้วออกทางประตู **Y** ให้เราเห็น เดี๋ยวเราเฝ้าดูจากข้างนอกนี้นี่แหละ*

ถ้าแบบนั้น ก็เท่ากับให้คำใบ้หนะสิ

เขาวงกต ▶ โจทย์



มา! เดี๋ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ -_-

เธอนี่เรื่องมากจังนะ :(จะเอาไง

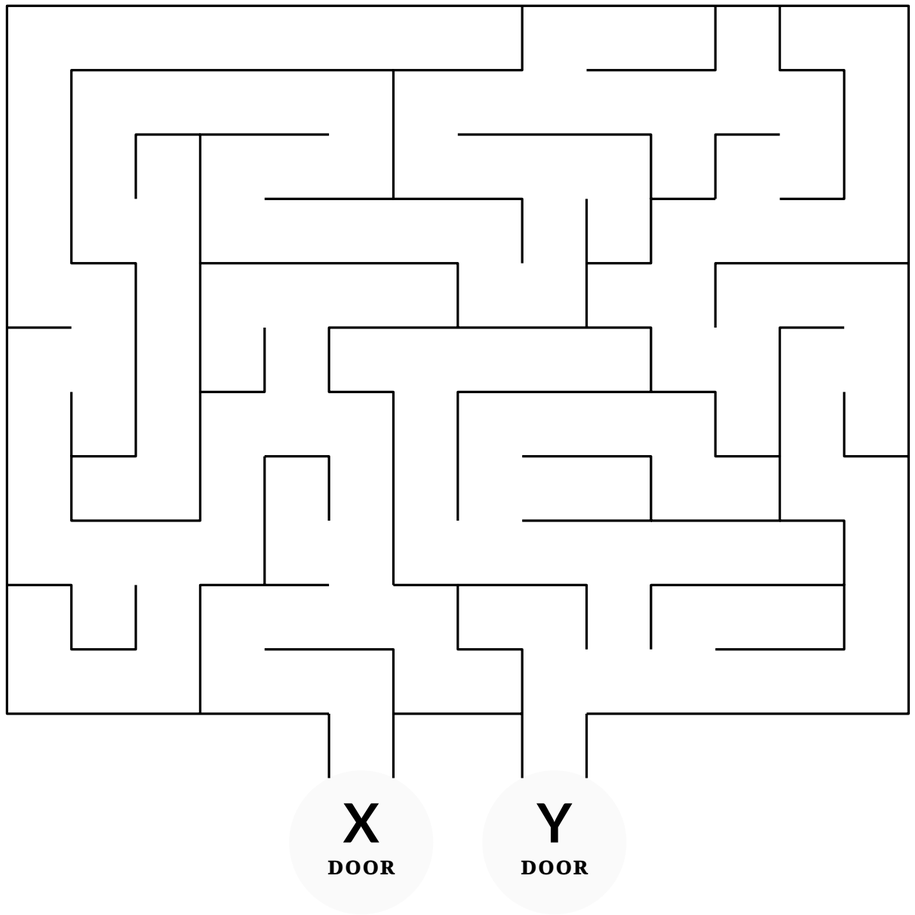
จริง ๆ มันก็มีวิธีอยู่นะ

แกก็เข้าประตู **X** ไป แล้วออกทางประตู **Y** ให้เราเห็น
เดี๋ยวเราเฝ้าดูจากข้างนอกนี้นี่แหละ

ถ้าแบบนั้น ก็เท่ากับให้คำใบ้หนะสิ

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

เขาวงกต ▶ โจทย์



ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ -_-

เธอนี่เรื่องมากจังนะ :(จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

แกก็เข้าประตู **X** *ไป แล้วออกทางประตู* **Y** *ให้เราเห็น เดี๋ยวเราเฝ้าดูจากข้างนอกนี้นี่แหละ*

ถ้าแบบนั้น ก็เท่ากับให้คำใบ้หนะสิ

. . . ว่ามีทางเข้า–ออกเขาวงกต ที่ต้องเข้าจากประตู **X** *แล้วออกทางประตู* **Y**

เธอไม่ควรรู้ด้วยซ้ำว่ามีเส้นทางแบบนั้น มันก็คือสปอยล์รูปแบบหนึ่งนะ

Zero-Knowledge Proof

Zero-Knowledge Proof

เป้าหมายการสื่อสาร **พิสูจน์ข้อเท็จจริง**บางอย่างให้อีกฝ่ายทราบ

Zero-Knowledge Proof

เป้าหมายการสื่อสาร **พิสูจน์ข้อเท็จจริง**บางอย่างให้อีกฝ่ายทราบ

เงื่อนไข ผู้ฟังต้อง**ไม่เรียนรู้สิ่งอื่นใด**นอกเหนือจากว่าข้อเท็จจริงถูกต้อง

Zero-Knowledge Proof

เป้าหมายการสื่อสาร **พิสูจน์ข้อเท็จจริง**บางอย่างให้อีกฝ่ายทราบ

เงื่อนไข ผู้ฟังต้อง**ไม่เรียนรู้สิ่งอื่นใด**นอกเหนือจากว่าข้อเท็จจริงถูกต้อง

เช่น พิสูจน์ว่า **บางปัญหามีคำตอบ** แต่ ไม่บอกคำตอบ ✔

Zero-Knowledge Proof

เป้าหมายการสื่อสาร **พิสูจน์ข้อเท็จจริง**บางอย่างให้อีกฝ่ายทราบ

เงื่อนไข ผู้ฟังต้อง**ไม่เรียนรู้สิ่งอื่นใด**นอกเหนือจากว่าข้อเท็จจริงถูกต้อง

เช่น พิสูจน์ว่า **บางปัญหามีคำตอบ** แต่ ไม่บอกคำตอบ ✔

พิสูจน์ว่า **ฉันอายุ 18 ปีขึ้นไป** แต่ ไม่บอกวัน-เดือน-ปีเกิด 📅

Zero-Knowledge Proof

เป้าหมายการสื่อสาร **พิสูจน์ข้อเท็จจริง**บางอย่างให้อีกฝ่ายทราบ

เงื่อนไข ผู้ฟังต้อง**ไม่เรียนรู้สิ่งอื่นใด**นอกเหนือจากว่าข้อเท็จจริงถูกต้อง

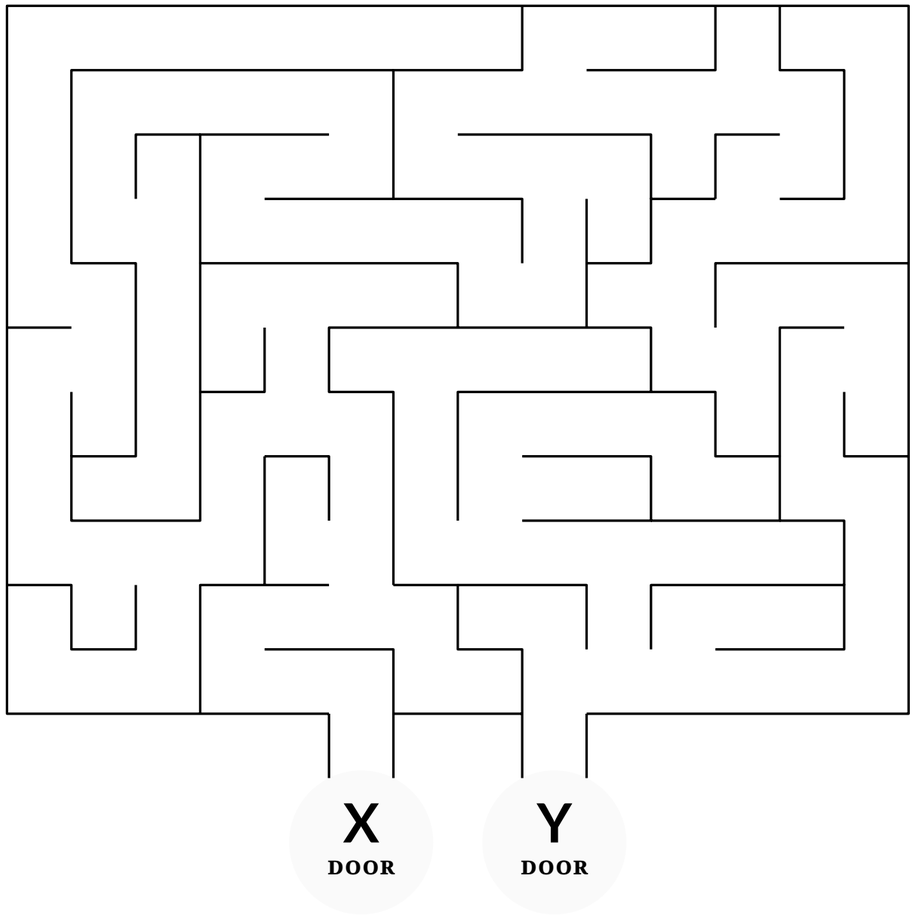
เช่น พิสูจน์ว่า **บางปัญหามีคำตอบ** แต่ ไม่บอกคำตอบ ✔

พิสูจน์ว่า **ฉันอายุ 18 ปีขึ้นไป** แต่ ไม่บอกวัน-เดือน-ปีเกิด 📅

พิสูจน์ว่า **ฉันมีสิทธิเข้าถึงข้อมูล** แต่ ไม่บอก credentials / secret key 🔑

~~พิสูจน์ว่า **บางปัญหาแก้ไขได้** แต่ ไม่บอกวิธีแก้ไข~~ 😊

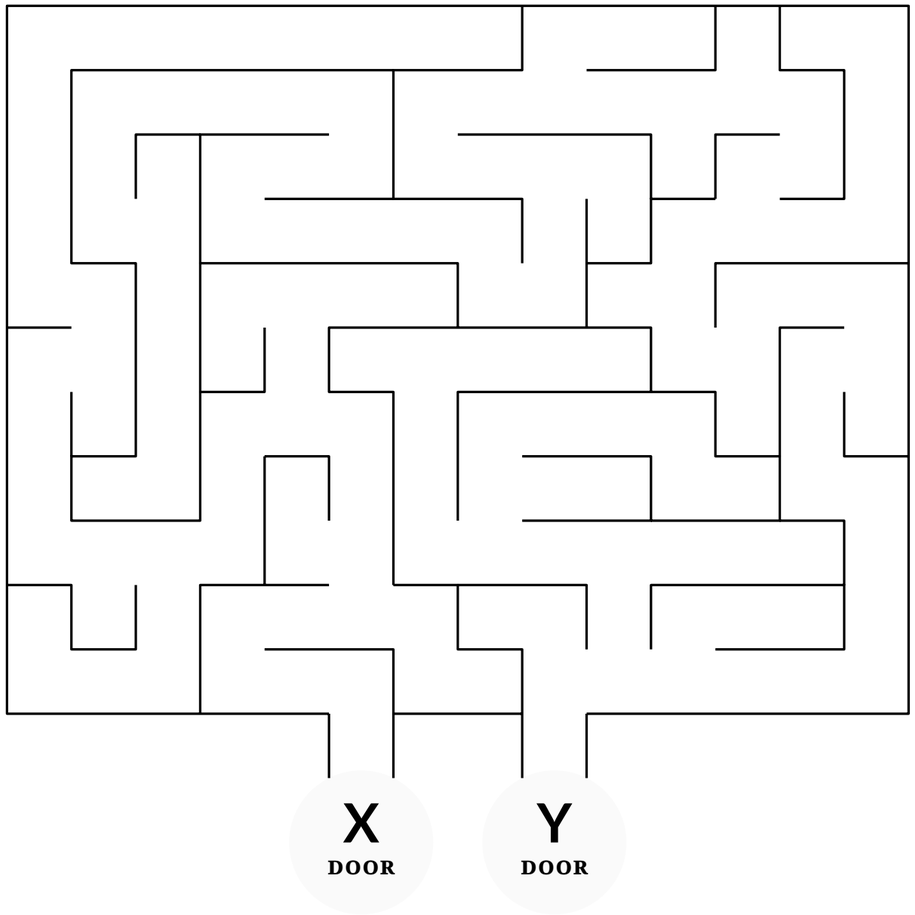
เขาวงกต ▶ วิธีแก้ปัญหา



Alice ผู้พิสูจน์

ผู้ตรวจสอบ **Bob**

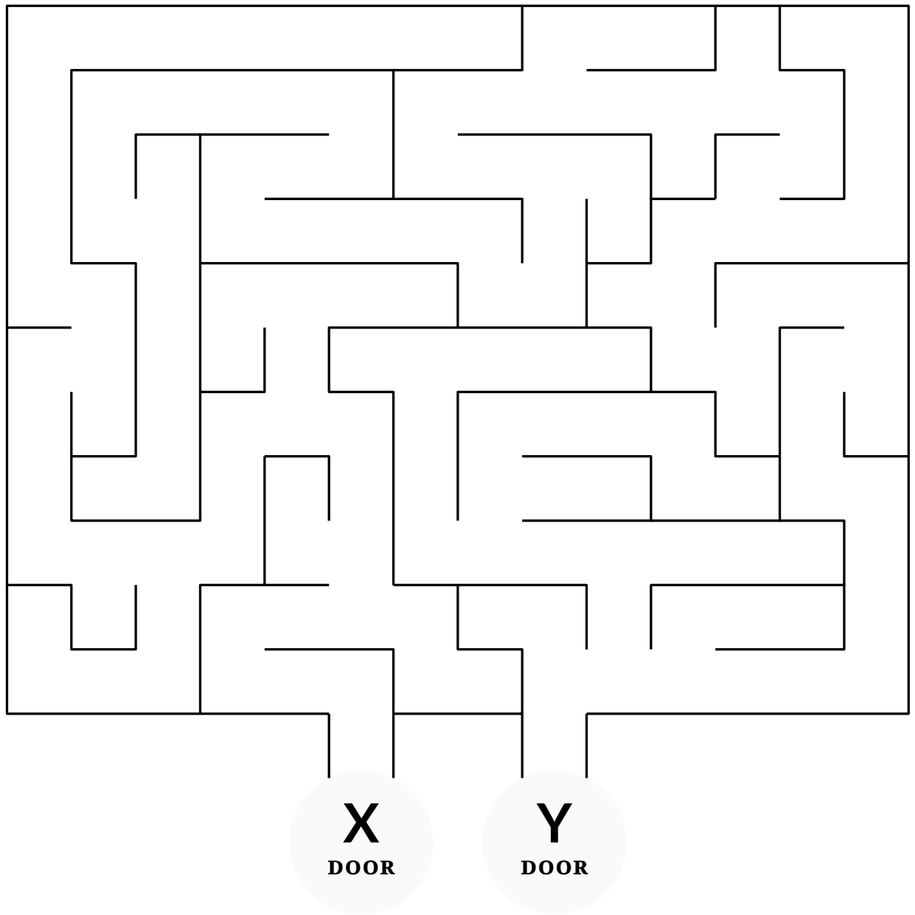
เขาวงกต ▶ วิธีแก้ปัญหา



Alice ผู้พิสูจน์ — ผู้ตรวจสอบ **Bob**

เอาอย่างนี้แล้วกัน (1) เดี๋ยวเธอหันหลังก่อน แล้วฉันจะเดินเข้าไปเตรียมตัวข้างใน จากนั้น (2) เดี๋ยวฉันจะเดินออกมาให้เธอดู

เขาวงกต ▶ วิธีแก้ปัญหา

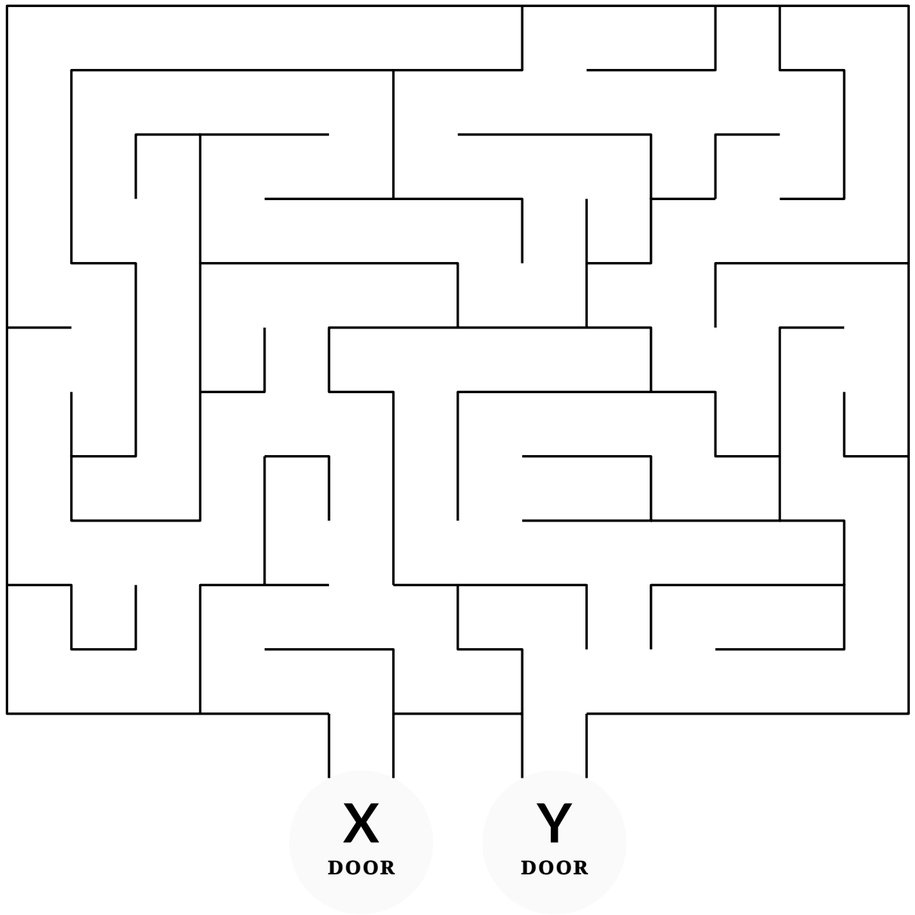


Alice ผู้พิสูจน์ — ผู้ตรวจสอบ **Bob**

เอาอย่างนี้แล้วกัน (1) เดี๋ยวเธอหันหลังก่อน แล้วฉันจะเดินเข้าไปเตรียมตัวข้างใน จากนั้น (2) เดี๋ยวฉันจะเดินออกมาให้เธอดู

ทำแบบนี้แล้วเธอก็ไม่รู้ว่าฉันเดินเข้าประตูไหน

เขาวงกต ▶ วิธีแก้ปัญหา



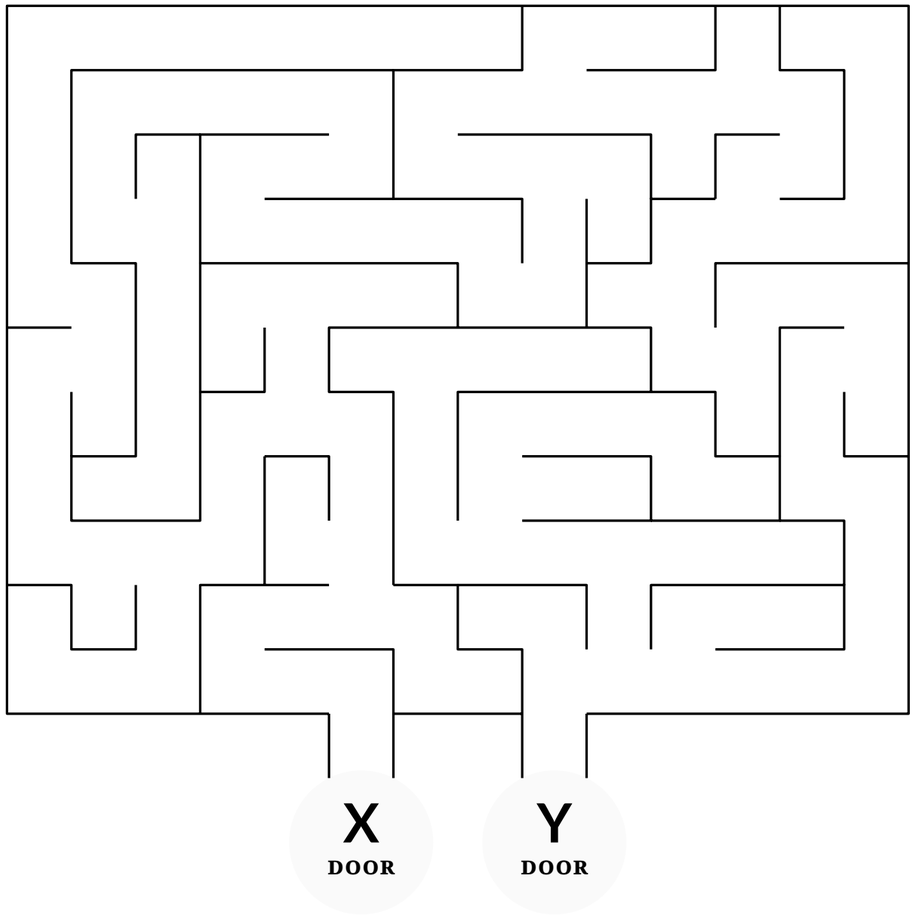
Alice ผู้พิสูจน์ — ผู้ตรวจสอบ **Bob**

เอาอย่างนี้แล้วกัน (1) เดี๋ยวเธอหันหลังก่อน แล้วฉันจะเดินเข้าไปเตรียมตัวข้างใน จากนั้น (2) เดี๋ยวฉันจะเดินออกมาให้เธอดู

ทำแบบนี้แล้วเธอก็ไม่รู้ว่าฉันเดินเข้าประตูไหน

อ้าว! แล้วแบบนี้จะรู้ได้ไงว่าแกไม่ได้กลับออกมาทางเดิมที่แกเดินเข้าไป

เขาวงกต ▶ วิธีแก้ปัญหา



Alice ผู้พิสูจน์ — ผู้ตรวจสอบ **Bob**

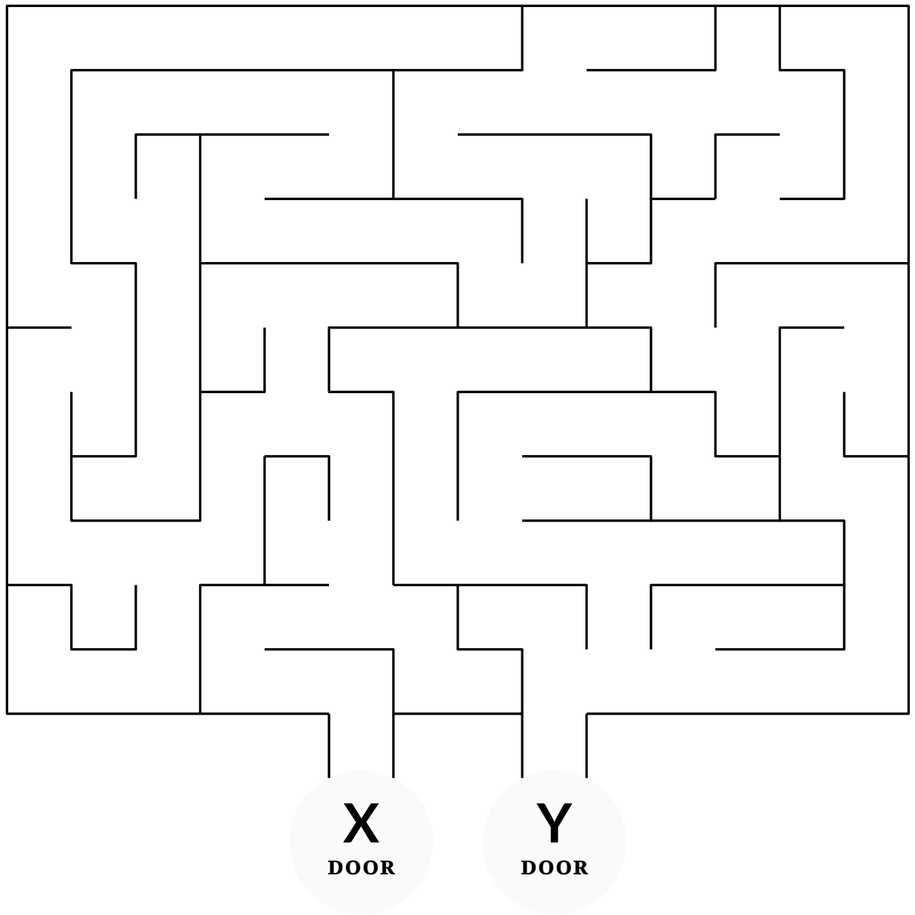
เอาอย่างนี้แล้วกัน (1) เดี๋ยวเธอหันหลังก่อน แล้วฉันจะเดินเข้าไปเตรียมตัวข้างใน จากนั้น (2) เดี๋ยวฉันจะเดินออกมาให้เธอดู

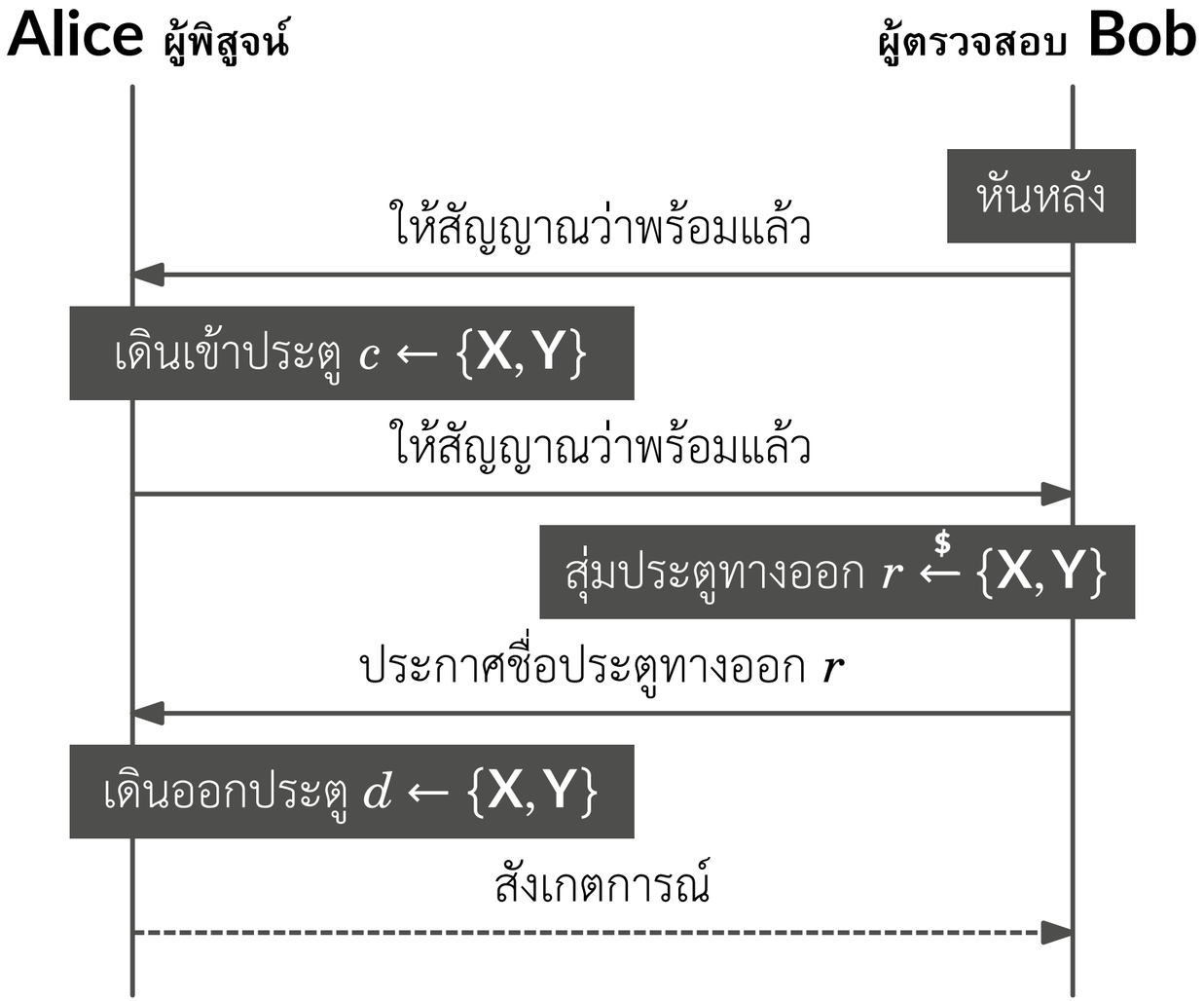
ทำแบบนี้แล้วเธอก็ไม่รู้ว่าฉันเดินเข้าประตูไหน

อ้าว! แล้วแบบนี้จะรู้ได้ไงว่าแกไม่ได้กลับออกมาทางเดิมที่แกเดินเข้าไป

เธอก็สุ่มสิว่าจะให้ฉันเดินออกทางประตูไหน ถ้าฉันรู้วิธีแก้เขาวงกต ฉันจะเดินออกประตูไหนก็ได้ / แต่ถ้าฉันไม่รู้ ฉันต้องเดาใจเธอไง

เขาวงกต ▶ วิธีแก้ปัญหา





THE HEART OF
Zero-Knowledge Proof

THE HEART OF
Zero-Knowledge Proof

COMPLETENESS

ถ้า **Alice** ทราบคำตอบจริง

แล้ว **Alice** สามารถพิสูจน์ว่า
ตนรู้จริงให้ **Bob** กระจ่างได้

THE HEART OF
Zero-Knowledge Proof

COMPLETENESS

ถ้า **Alice** ทราบคำตอบจริง

แล้ว **Alice** สามารถพิสูจน์ว่าตนรู้จริงให้ **Bob** กระจ่างได้

SOUNDNESS

ถ้า **Alice** ไม่ทราบคำตอบ

แล้ว **Alice** ไม่สามารถหลอกให้ **Bob** เชื่อคล้อยตามได้

THE HEART OF
Zero-Knowledge Proof

COMPLETENESS

ถ้า **Alice** ทราบคำตอบจริง

แล้ว **Alice** สามารถพิสูจน์ว่าตนรู้จริงให้ **Bob** กระจ่างได้

SOUNDNESS

ถ้า **Alice** ไม่ทราบคำตอบ

แล้ว **Alice** ไม่สามารถหลอกให้ **Bob** เชื่อคล้อยตามได้

ZERO-KNOWLEDGE

ถ้า **Alice** ทราบคำตอบจริง

แล้ว **Bob** ไม่ได้เรียนรู้สิ่งใดจาก **Alice** เว้นเฉพาะสิ่งที่ **Bob** คาดเดาได้ด้วยตัวเอง

THE HEART OF
Zero-Knowledge Proof

CORRECTNESS PROPERTY

COMPLETENESS

ถ้า **Alice** ทราบคำตอบจริง

แล้ว **Alice** สามารถพิสูจน์ว่าตนรู้จริงให้ **Bob** กระจ่างได้

**ด้วยความน่าจะเป็นที่สูงมาก ๆ*

SOUNDNESS

ถ้า **Alice** ไม่ทราบคำตอบ

แล้ว **Alice** ไม่สามารถหลอกให้ **Bob** เชื่อคล้อยตามได้

**ด้วยความน่าจะเป็นที่สูงมาก ๆ*

SECURITY PROPERTY

ZERO-KNOWLEDGE

ถ้า **Alice** ทราบคำตอบจริง

แล้ว **Bob** ไม่ได้เรียนรู้สิ่งใดจาก **Alice** เว้นเฉพาะสิ่งที่ **Bob** คาดเดาได้ด้วยตัวเอง

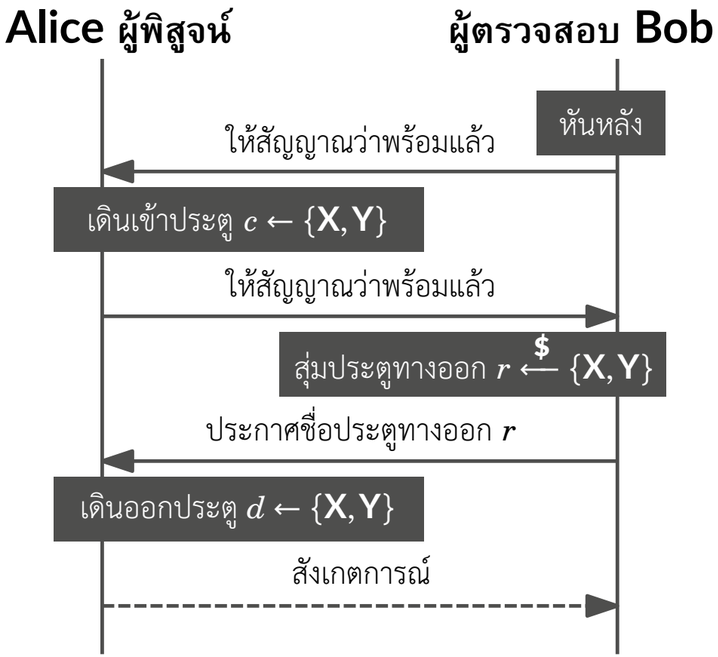
**ด้วยความน่าจะเป็นที่สูงมาก ๆ*

เขาวงกต ▶ ประเมินวิธีแก้ปัญหา

COMPLETENESS

SOUNDNESS

ZERO-KNOWLEDGE

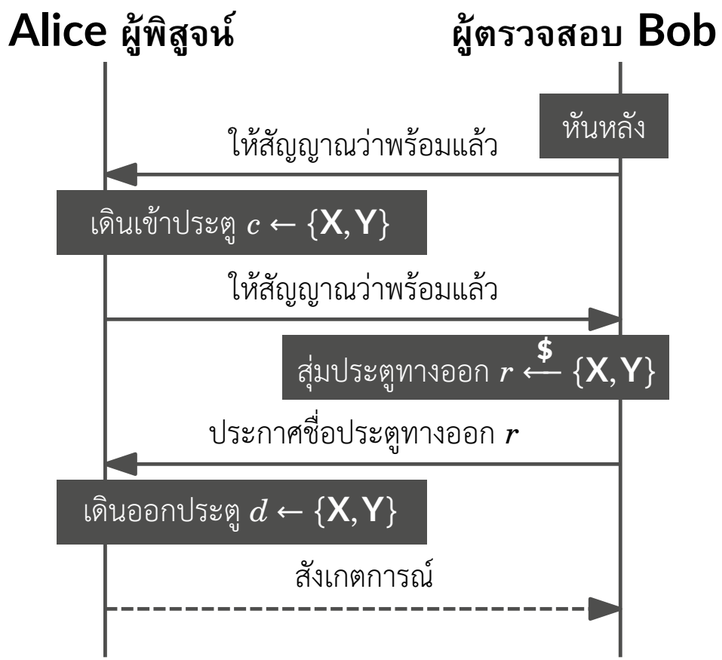


เขาวงกต ▶ ประเมินวิธีแก้ปัญหา

COMPLETENESS

SOUNDNESS

ZERO-KNOWLEDGE



ถ้า **Alice** ทราบคำตอบจริง

(**Alice** รู้เส้นทางระหว่างประตูทั้งสอง)

⇓

Alice สามารถเลือกออกประตูไหนก็ได้

⇓

Alice สามารถเลือกออกประตูที่ **Bob** กำหนดให้ได้เสมอ

เพียงแค่เลือก $d = r$

⇓

Bob เชื่อว่า **Alice** ทราบคำตอบจริง

(ด้วยความน่าจะเป็น เท่ากับ 100%)

⇓

แล้ว **Alice** สามารถพิสูจน์ว่าตนรู้จริงให้ **Bob** กระจ่างได้

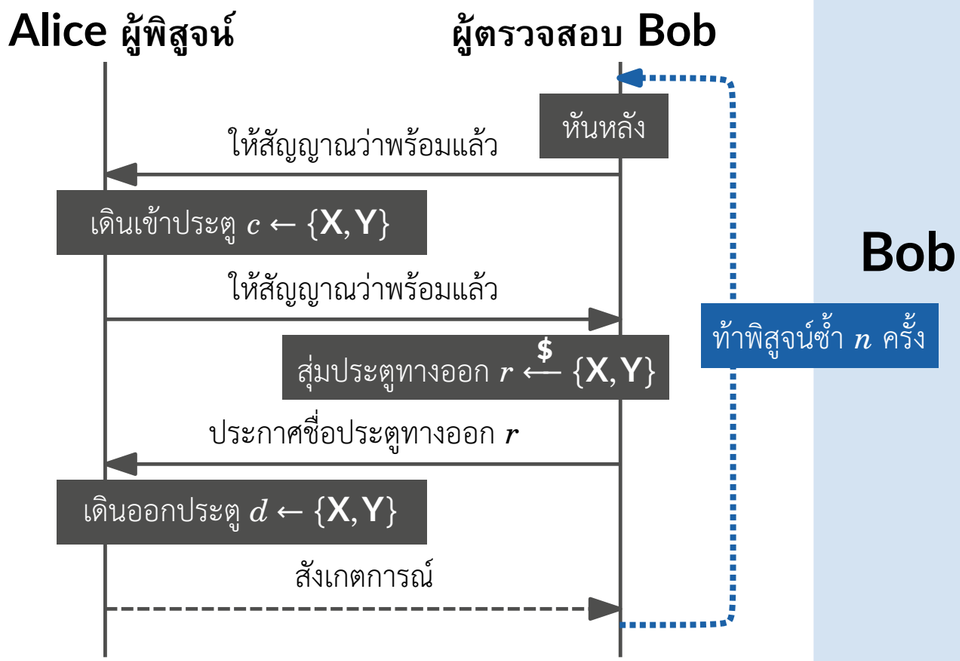
(ด้วยความน่าจะเป็น เท่ากับ 100%)

เขาวงกต ▶ ประเมินวิธีแก้ปัญหา

COMPLETENESS

SOUNDNESS

ZERO-KNOWLEDGE



ถ้า **Alice** ไม่ทราบคำตอบ

⇓

Alice จำเป็นต้องออกทางประตูที่เข้ามา

นั่นคือบังคับเลือก $d = c$

⇓

Alice ต้องเดาว่า **Bob** จะให้ออกประตูใด

โอกาสเดา $c = r$ ถูกต้องเพียง 50% เปอร์เซ็นต์

⇓

Bob สามารถท้า **Alice** พิสูจน์ซ้ำได้**หลายครั้ง** เผื่อ(บางครั้ง)ถูกหลอก

โอกาสที่ **Bob** ถูกหลอกสำเร็จติดกันจะลดลง และความเชื่อมั่นก็จะมากขึ้น

(เช่น ถ้าทดสอบ $n = 20$ ครั้ง ความมั่นใจจะเพิ่มเป็น $1 - 0.5^n \approx 99.999905\%$)

⇓

แล้ว **Alice** ไม่สามารถหลอกให้ **Bob** เชื่อคล้อยตามได้

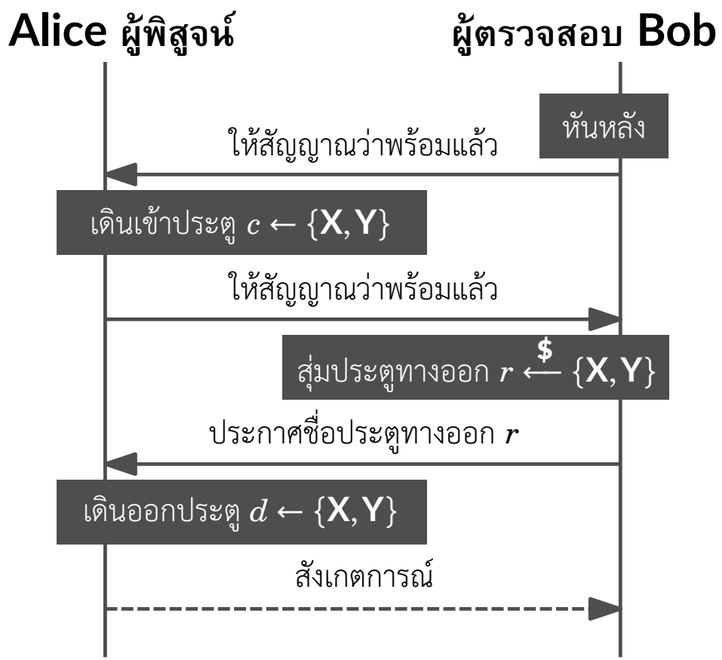
(ด้วยความน่าจะเป็น มากกว่า 99.99%)

เขาวงกต ▶ ประเมินวิธีแก้ปัญหา

COMPLETENESS

SOUNDNESS

ZERO-KNOWLEDGE



ถ้า **Alice** ทราบคำตอบจริง

(**Alice** รู้เส้นทางระหว่างประตูทั้งสอง)

Alice สามารถเลือกออกประตู ที่ **Bob** กำหนดให้ได้เสมอ

ถึงแม้สมมติ **Alice** ไม่อยู่ **Bob** สามารถ**ลองจินตนาการ**ได้

Bob จะเห็นภาพ **Alice** เดินออกทางประตูที่ตนเรียกเสมอ

แล้ว **Bob** ไม่ได้เรียนรู้สิ่งใดจาก **Alice** เว้นเฉพาะสิ่งที่ **Bob** คาดเดาได้ด้วยตัวเอง

ลายเซ็นดิจิทัล ▶ วิเคราะห์

ข้อมูลเบื้องต้น FIDO Alliance นำเสนอวิธีใช้ Digital Signature เพื่อ**พิสูจน์ตัวตน (Authentication)** ผ่านเว็บไซต์

fido™ ALLIANCE | simpler stronger authentication

https://fidoalliance.org/

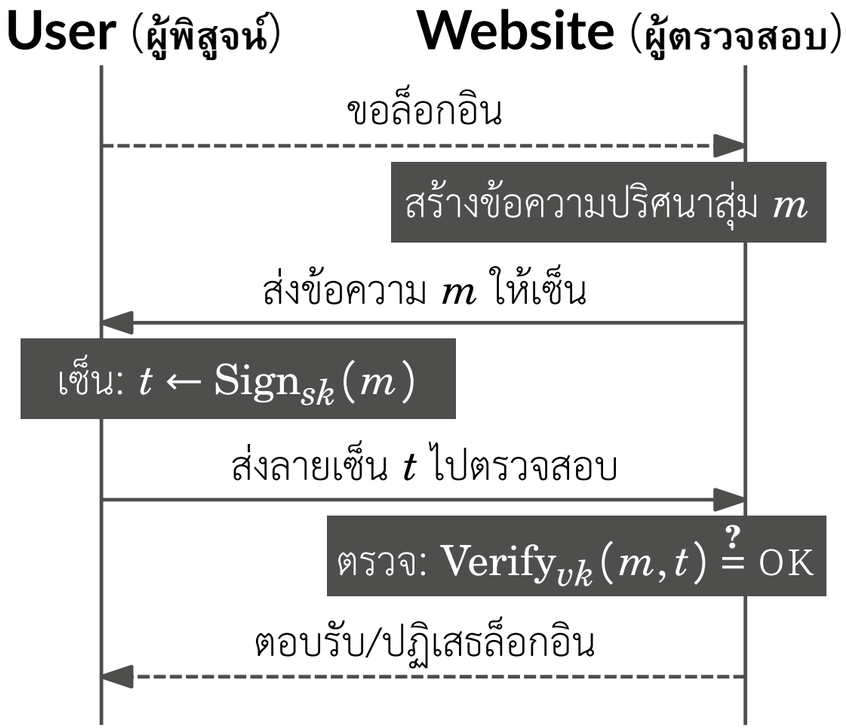
ลายเซ็นดิจิทัล ▶ วิเคราะห์

ข้อมูลเบื้องต้น FIDO Alliance นำเสนอวิธีใช้ Digital Signature เพื่อ**พิสูจน์ตัวตน (Authentication)** ผ่านเว็บไซต์

fido ALLIANCE simpler stronger authentication

https://fidoalliance.org/

จงพิสูจน์**ความเป็นเจ้าของ**กุญแจสาธารณะ (verification key, vk) โดยใช้กุญแจส่วนตัว (signing key, sk) เซ็นข้อความปริศนาที่กำหนดให้



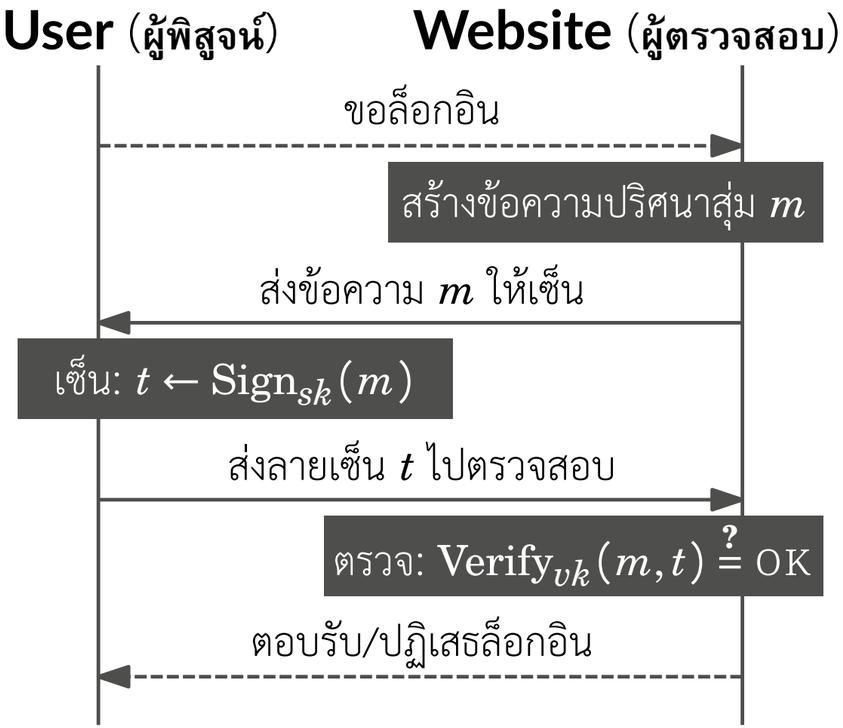
ลายเซ็นดิจิทัล ▶ วิเคราะห์

ข้อมูลเบื้องต้น FIDO Alliance นำเสนอวิธีใช้ Digital Signature เพื่อ**พิสูจน์ตัวตน (Authentication)** ผ่านเว็บไซต์

fido ALLIANCE simpler stronger authentication

https://fidoalliance.org/

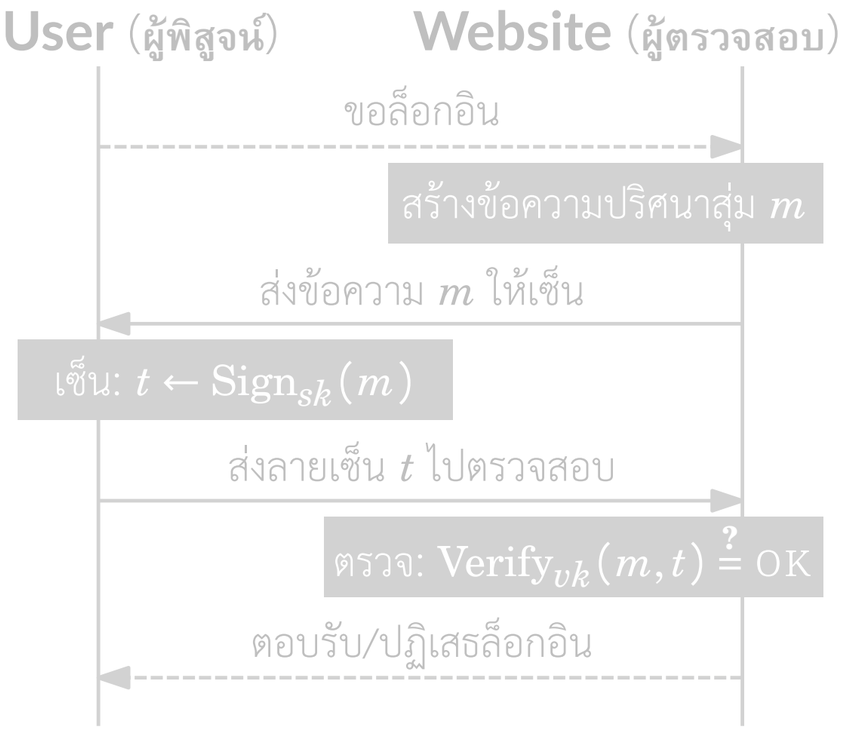
จงพิสูจน์**ความเป็นเจ้าของ**กุญแจสาธารณะ (verification key, vk) โดยใช้กุญแจส่วนตัว (signing key, sk) เซ็นข้อความปริศนาที่กำหนดให้



IS THIS PROTOCOL ZERO-KNOWLEDGE?

NO

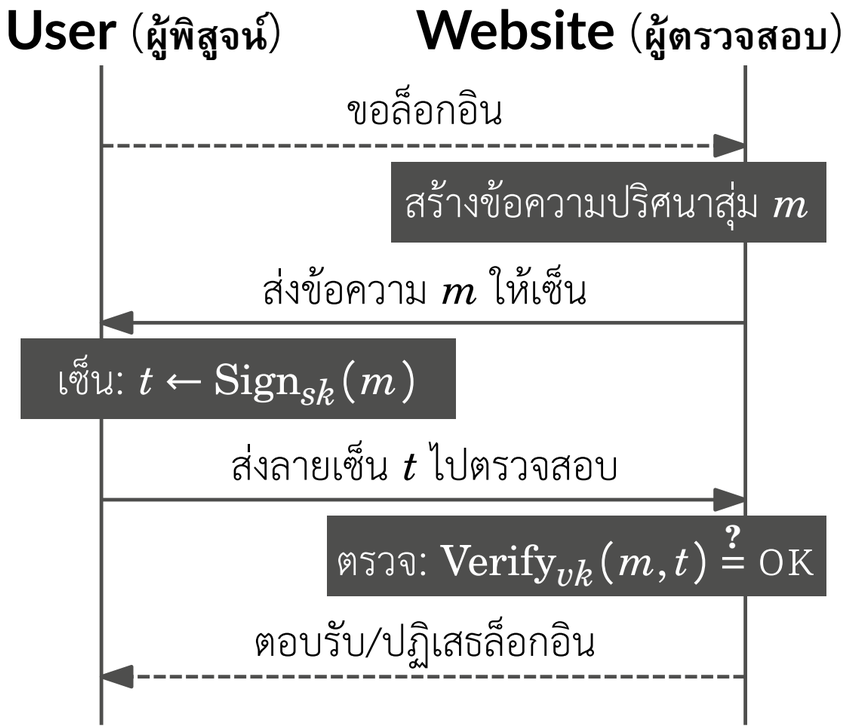
IS THIS PROTOCOL ZERO-KNOWLEDGE?



NO

IS THIS PROTOCOL ZERO-KNOWLEDGE?

เหตุผล **Website** ไม่สามารถคาดเดาลายเซ็น t ได้ด้วยตัวเอง (แต่เรียนรู้ได้จาก **User**)



ตัวอย่าง ▶ ซูโดกุ

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

ปัญหาซูโดกุ

ตัวอย่าง ▶ ซูโดกุ

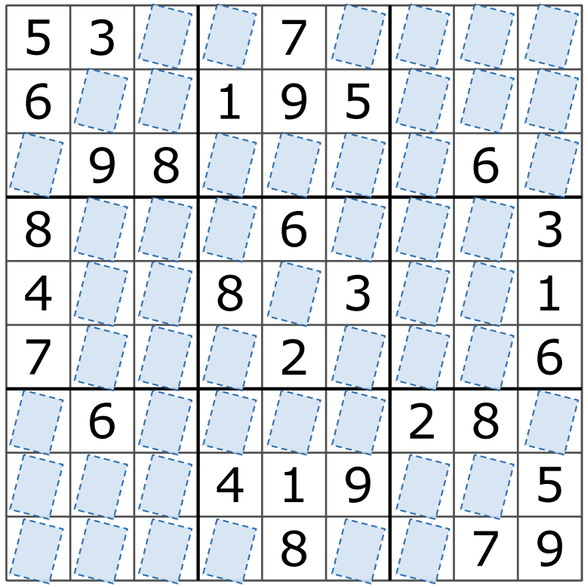
5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

ปัญหาซูโดกุ

IMAGE SOURCE https://commons.wikimedia.org/wiki/File:Sudoku_Puzzle_by_L2G-20050714_standardized_layout.svg

ต้องการพิสูจน์ว่าปริศนานี้ **มีคำตอบ**
แต่**ไม่บอก**คำตอบ

ตัวอย่าง ▶ ซูโดกุ



ปัญหาซูโดกุ

IMAGE SOURCE https://commons.wikimedia.org/wiki/File:Sudoku_Puzzle_by_L2G-20050714_standardized_layout.svg

ต้องการพิสูจน์ว่าปริศนานี้ **มีคำตอบ**
แต่**ไม่บอก**คำตอบ

- https://medium.com/qed-it/the-incredible-machine-4d1270d7363a
- http://www.wisdom.weizmann.ac.il/~naor/PAPERS/SUDOKU_DEMO

Act II

OUT IN THE FIELDS

ตัวอย่าง ▶ บล็อกเชน

Cryptocurrency

Generic

zk-SNARKs protocol

ตัวอย่าง ▶ บล็อกเชน

Cryptocurrency

Generic

$$\text{เงินโอน}_1 + \text{เงินโอน}_2 + \ldots + \text{เงินโอน}_m = \text{เงินรับ}_1 + \text{เงินรับ}_2 + \ldots + \text{เงินรับ}_k$$

zk-SNARKs protocol

ตัวอย่าง ▶ บล็อกเชน

Cryptocurrency

Generic

QED it

$$\text{เงินโอน}_1 + \text{เงินโอน}_2 + \ldots + \text{เงินโอน}_m = \text{เงินรับ}_1 + \text{เงินรับ}_2 + \ldots + \text{เงินรับ}_k$$

ซึ่งต้องพิสูจน์ สมการโอน-รับเงิน เป็นจริง $^+$ เงินแต่ละก้อน มีค่าเป็นบวก

เงื่อนไข ซ่อนมูลค่าเงินแต่ละก้อน

zk-SNARKs protocol

ตัวอย่าง ▶ บล็อกเชน

Cryptocurrency

Generic

$$\text{เงินโอน}_1 + \text{เงินโอน}_2 + \ldots + \text{เงินโอน}_m = \text{เงินรับ}_1 + \text{เงินรับ}_2 + \ldots + \text{เงินรับ}_k$$

ซึ่งต้องพิสูจน์

- สมการโอน-รับเงิน เป็นจริง
- $^{+}$ เงินแต่ละก้อน มีค่าเป็นบวก

เงื่อนไข

- ซ่อนมูลค่าเงินแต่ละก้อน
- ซ่อนเจ้าของบัญชี

zk-SNARKs protocol

ตัวอย่าง ▶ ยืนยันคุณสมบัติโดยไม่ระบุตัวตน

🏁 พิสูจน์ว่า **ฉันอายุ 18 ปีขึ้นไป** แต่ ไม่บอกวัน-เดือน-ปีเกิด

ตัวอย่าง ▶ ยืนยันคุณสมบัติโดยไม่ระบุตัวตน

🏁 พิสูจน์ว่า **ฉันอายุ 18 ปีขึ้นไป** แต่ ไม่บอกวัน-เดือน-ปีเกิด

IMAGE SOURCE http://www.richardbarrow.com/2011/07/thai-signs-cigarettes-sold-here/

ตัวอย่าง ▶ ยืนยันคุณสมบัติโดยไม่ระบุตัวตน

🏁 พิสูจน์ว่า **ฉันอายุ 18 ปีขึ้นไป** แต่ ไม่บอกวัน-เดือน-ปีเกิด

IMAGE SOURCE http://www.richardbarrow.com/2011/07/thai-signs-cigarettes-sold-here/

$$\textit{เวลาปัจจุบัน} - \textit{เวลาเกิด} \geq \text{“18 ปี”}$$

ตัวอย่าง ▶ ยืนยันคุณสมบัติโดยไม่ระบุตัวตน

🏁 พิสูจน์ว่า **ฉันอายุ 18 ปีขึ้นไป** แต่ ไม่บอกวัน-เดือน-ปีเกิด

IMAGE SOURCE http://www.richardbarrow.com/2011/07/thai-signs-cigarettes-sold-here/

เวลาปัจจุบัน − *เวลาเกิด* ≥ “18 ปี”

ซึ่งต้องพิสูจน์ อสมการเป็นจริง

เงื่อนไข ซ่อนวัน-เดือน-ปีเกิด/อายุ

และอื่น ๆ อีกมากมาย

ตัวอย่าง ▶ ยืนยันคุณสมบัติโดยไม่ระบุตัวตน

Attribute-based Credentials

Microsoft U-Prove

IBM Bluemix

Identity Mixer

Radboud Universiteit Nijmegen

IRMA Project

🏁 พิสูจน์ว่า **ฉันอายุ 18 ปีขึ้นไป** แต่ ไม่บอกวัน-เดือน-ปีเกิด

IMAGE SOURCE http://www.richardbarrow.com/2011/07/thai-signs-cigarettes-sold-here/

เวลาปัจจุบัน − เวลาเกิด ≥ "18 ปี"

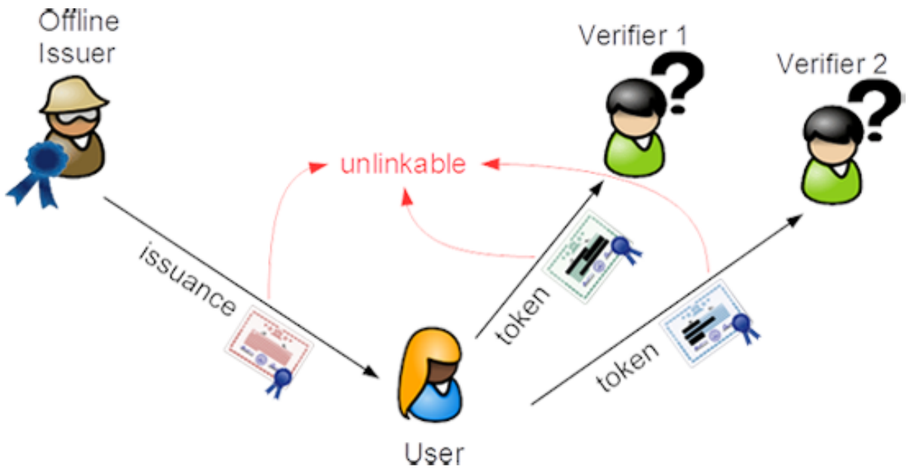
ซึ่งต้องพิสูจน์ — อสมการเป็นจริง

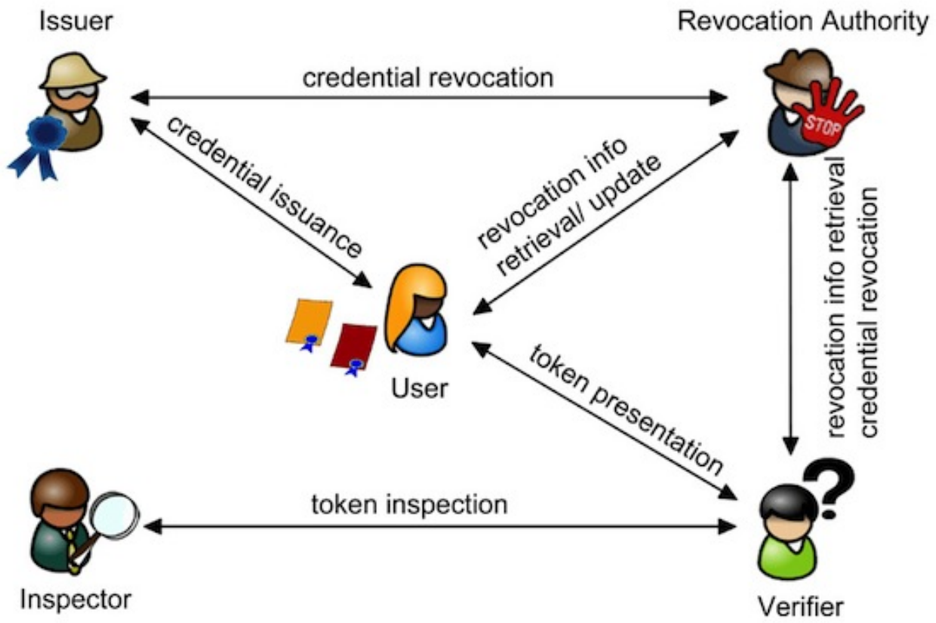
เงื่อนไข — ซ่อนวัน-เดือน-ปีเกิด/อายุ

และอื่น ๆ อีกมากมาย

ตัวอย่าง ▶ ยืนยันคุณสมบัติโดยไม่ระบุตัวตน (เมื่อกี้ยังไม่จบ)

IBM Bluemix





ATTRIBUTE PREDICATES
MULTI-CREDENTIAL TOKENS
REVOCATION
INSPECTION
SCOPE-EXCLUSIVE PSEUDONYMS
ADVANCED ISSUANCE

https://www.zurich.ibm.com/identity_mixer/

Act III

SIBLINGS OF ZK PROOFS IN CRYPTOG–RAPHY

Secure Multi – Party Computation

การคำนวณร่วมพหุภาคี

Secure Multi – Party Computation

การคำนวณร่วมพหุภาคี

เป้าหมายการสื่อสาร **คำนวณผลลัพธ์**ร่วมกัน จากข้อมูลลับของแต่ละคน

เงื่อนไข ผู้เล่นแต่ละคน**ไม่เรียนรู้ข้อมูลลับ**ของผู้อื่น

Secure Multi – Party Computation

การคำนวณร่วมพหุภาคี

เป้าหมายการสื่อสาร คำนวณผลลัพธ์ร่วมกัน จากข้อมูลลับของแต่ละคน

เงื่อนไข ผู้เล่นแต่ละคนไม่เรียนรู้ข้อมูลลับของผู้อื่น

ตัวอย่าง 

$$\underset{\text{ผลลัพธ์}}{\textit{ค่าเฉลี่ยน้ำหนัก}} = \frac{1}{n} \cdot \textbf{ผลรวม}(\underset{\text{ความลับ}}{\textit{น้ำหนัก}_1}, \underset{\text{ความลับ}}{\textit{น้ำหนัก}_2}, \ldots, \underset{\text{ความลับ}}{\textit{น้ำหนัก}_n})$$

Secure Multi – Party Computation

การคำนวณร่วมพหุภาคี

เป้าหมายการสื่อสาร คำนวณผลลัพธ์ร่วมกัน จากข้อมูลลับของแต่ละคน

เงื่อนไข ผู้เล่นแต่ละคนไม่เรียนรู้ข้อมูลลับของผู้อื่น

ตัวอย่าง

$$\underbrace{\textit{ค่าเฉลี่ยน้ำหนัก}}_{\text{ผลลัพธ์}} = \frac{1}{n} \cdot \textbf{ผลรวม}(\underbrace{\textit{น้ำหนัก}_1}_{\text{ความลับ}}, \underbrace{\textit{น้ำหนัก}_2}_{\text{ความลับ}}, \ldots, \underbrace{\textit{น้ำหนัก}_n}_{\text{ความลับ}})$$

Secure Voting

(Fully) Homomorphic Encryption

การเข้ารหัสแบบสาทิสสัณฐาน

(Fully) Homomorphic Encryption

การเข้ารหัสแบบสาทิสสัณฐาน

เป้าหมายการสื่อสาร **คำนวณผลลัพธ์**จากข้อมูลที่ถูกเข้ารหัส

เงื่อนไข โดย**ไม่จำเป็นต้องถอดรหัส**

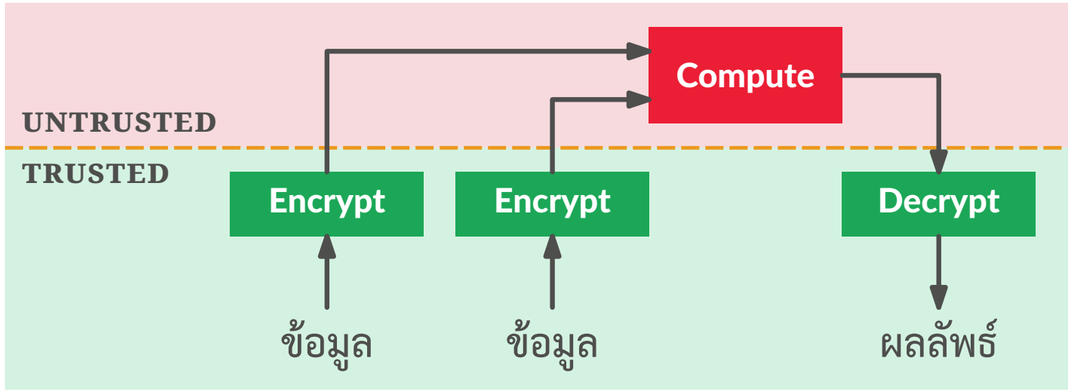
(Fully) Homomorphic Encryption

การเข้ารหัสแบบสาทิสสัณฐาน

เป้าหมายการสื่อสาร คำนวณผลลัพธ์จากข้อมูลที่ถูกเข้ารหัส

เงื่อนไข โดยไม่จำเป็นต้องถอดรหัส

ตัวอย่าง



- **Encryption in Cloud Services**
- **Searchable Encrypted Databases**

Q & A

https://forms.office.com/Pages/ResponsePage.aspx?id=n98RjhVGT0OmxooMtP_rbEMN0M1iPkBBiRj9xXWk0qBURU9LVU01OVg1U1lKSzlUMzg3RjFKVVBGMi4u&qrcode=true