from a given country — have two key flaws. First, these decisions are made about entire countries, rather than individuals, disregarding vast differences between people within countries. Second, they are typically made on the basis of country-level epidemiological data that, as the present study shows, have notable shortcomings.

Had border agents denied entry to all passengers from countries that had concerning metrics, they would have prevented those people with COVID-19 from entering Greece — but at the cost of crushing a key pillar of the economy. Had they simply tested people proportional to a country's reported COVID-19 metrics rather than algorithmic predictions, however, their testing efficiency would have been much lower. This is because reported COVID-19 metrics can be very different from actual disease prevalence among incoming travellers. Travellers are not randomly drawn from their countries' populations, and passively collected data on cases of COVID-19 or deaths associated with the disease reflect large reporting biases and systemic barriers to access[7].

Indeed, by efficiently testing incoming passengers, the authors' algorithm was able to anticipate spikes in SARS-CoV-2 infection rates among traveller populations almost 9 days earlier than if they had used country-level epidemiological data alone. This indicates the enormous value of intelligent, deliberate data collection — and the dangers of relying on blunt, flawed, country-level data for important decisions.

Bastani and colleagues' work will be remembered as one of the best examples of using data in the fight against COVID-19. It is a compelling story of how a group of researchers partnered with enlightened policymakers to produce a tool that has enormous social value. It highlights the best parts of both academic research and the civil service, and shows the great promise of artificial intelligence for making good decisions — which in many settings can be the difference between life and death.

Ziad Obermeyer is in the Division of Health Policy and Management, School of Public Health, University of California, Berkeley, Berkeley, California 94720, USA.
e-mail: zobermeyer@berkeley.edu

1. Bastani, H. *et al. Nature* **599**, 108–113 (2021).
2. Marmot, M. & Wilkinson, R. (eds) *Social Determinants of Health* (Oxford Univ. Press, 2005).
3. Mullainathan, S. & Obermeyer, Z. *Diagnosing Physician Error: A Machine Learning Approach to Low-Value Health Care*. National Bureau of Economic Research Working Paper 26168 (2021).
4. Thompson, W. R. *Biometrika* **25**, 285–294 (1933).
5. Silver, D. *et al. Nature* **529**, 484–489 (2016).
6. Li, L., Chu, W., Langford, J. & Schapire, R. E. in *Proc. 19th Int. Conf. World Wide Web* 661–670 (2010).
7. Wu, S. L. *et al. Nature Commun.* **11**, 4507 (2020).

The author declares no competing interests.
This article was published online on 22 September 2021.

Cryptography

Relativity could ensure security for cash machines

Gilles Brassard

Entering your personal identification number using the keypad of a cash machine is notoriously insecure. A clever application of the special theory of relativity could make identification safer. **See p.47**

When you type in your personal identification number (PIN) at a cash machine, you feel safe — provided you cover the keypad with your hand. But even the machines attached to banks are vulnerable to attack by fraudsters, some of whom go as far as to add fake machinery to legitimate machines as a way of stealing PINs (see go.nature.com/3p9r431). To prevent this type of fraud, a solution is needed that allows people to prove their identity without disclosing any secret information. On page 47, Alikhani *et al.*[1] describe an experiment that achieves this goal with unprecedented security, guaranteed by Albert Einstein's special theory of relativity.

The identification technique used by Alikhani and colleagues is an application of a concept known as a zero-knowledge proof[2]. Imagine that Alice wants to convince her friend Bob that she knows how to do something, but she wants to keep her technique secret. For example, suppose she is capable of distinguishing between two brands of cola in a glass simply by looking at them. She asks a sceptical Bob to switch around identical glasses containing the two types of cola while her back is turned. If she can still tell the drinks apart, and can repeat this feat several times, Bob will be convinced of her ability — but he won't have learnt how to do it himself. Alice has performed a zero-knowledge proof.

If Alice's trick relies on secret knowledge that is unique to her, then being able to do this task correctly functions like a cash-machine PIN for Alice's identity. Alice proves that she has information known only to her, but she doesn't share this information. So even if the cash machine is equipped with fake machinery, the person who installed it cannot later use what was learnt to impersonate Alice.

Remarkably, there is a zero-knowledge proof for any mathematical statement for which a conventional proof exists[3] — and there are highly efficient schemes for applying zero-knowledge proofs to the task of establishing someone's identity[4]. However, implementing a general zero-knowledge proof involves encoding the answers with an entirely different mathematical problem, such as factoring a large number. This means that the alleged security of most conventional zero-knowledge proofs[3,4] depends on how difficult this other mathematical problem is to solve. Unfortunately, once quantum computers are readily available, it will become possible to solve many of these other problems in a period of time that is sufficiently short to defeat the validity of the zero-knowledge proof[5].

To make a zero-knowledge proof unconditionally secure, Alice would need to prove her identity using two separate devices that cannot communicate with each other for the duration of her interaction with the bank[6]. This is similar to a detective interrogating two suspects in different rooms to determine the consistency of their joint alibi. Ideally, the two devices, provided by the bank, would require Alice to supply biometric information to activate them. They would be inserted into a pair of slots on the cash machine and perform zero-knowledge proofs on her behalf (Fig. 1). Because each of Alice's devices is kept ignorant of the questions asked of the other device, their answers will sometimes be inconsistent if they do not possess the secret they claim to have — that is, if they are fraudulent. But how can we be certain that the two devices cannot communicate with each other? This is where Einstein's special theory of relativity comes to the rescue.

Special relativity tells us that information cannot travel faster than light. Suppose Alice's two devices are one metre apart. Any signal requires more than 3.3 nanoseconds to travel between them. Therefore, if each device is required to respond within 3 ns of receiving their question, and if the questions are asked within a time window of 0.3 ns, the devices will be prevented from choosing their answers on the basis of the questions put to the other device. Such exquisite precision was thought to be technologically infeasible because it seemed to imply that an enormous amount of data would need to be communicated in this short time frame. However, a much

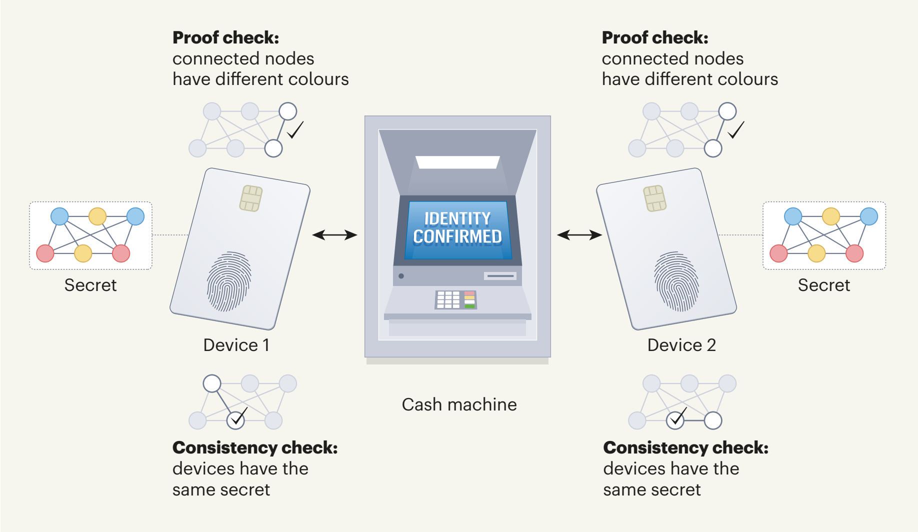

Figure 1 | An identification scheme using special relativity. Cash machines could perform identity checks that are based on the solution to a puzzle, such as the network used by Alikhani and co-workers[1]. Two devices share secret information that tells them how to colour a network's nodes so that no two connecting nodes have the same colour. The user activates the devices with a thumbprint, and the cash machine chooses two connected nodes and asks the devices to show that they have different colours. Answers are encoded so that the actual colours are revealed only when both devices are asked about the same node, and the colours are changed around to generate different solutions of the network puzzle between questions. These measures prevent fake machines from learning information to impersonate the user. Random 'trap' questions verify that the two devices' secret solutions are consistent. Repeating this process many times will expose fake devices, which would either assign the same colour to connected nodes or fail the consistency test. Limiting the time allowed for answers prevents the devices from helping each other to cheat, a consequence of Einstein's special theory of relativity.

more economical scheme[7] was proposed in 2020, which brings us to the work featured in Alikhani and co-workers' study.

The authors describe two implementations of a simplified version of the economical scheme proposed last year. In one experiment, the devices were placed at either end of a building at the University of Geneva in Switzerland and were separated by 60 metres – a distance that light takes 200 nanoseconds to travel. This is clearly an unreasonable distance to use in the cash-machine scenario, because it would require Alice's devices to be 60 metres apart. However, the authors argue that improvements within the reach of current technology would allow them to reduce this distance to only one metre. It is therefore possible to imagine Alice sliding her biometrically activated smart cards into two slots of the cash machine. It still might not be the most practical solution, but it is on the right track.

In addition to offering a promising approach to the conundrum of a secure cash machine, the work by Alikhani and colleagues succeeds in demonstrating a feasible relativistic zero-knowledge proof of a non-trivial mathematical statement. However, there are two theoretical caveats. First, the puzzle that Alice would be using to prove her identity could be solved by a malicious party that has sufficient computing power. And second, it might become possible for fraudsters to defeat the identification scheme by harnessing quantum entanglement[8], the mysterious property of quantum states that Einstein referred to as "spooky action at a distance". Although special relativity prevents the two devices from communicating quickly enough to fool a cash machine into mistaking them for Alice's devices, entanglement might allow the right correlations to appear instantaneously between the cheating devices with no need to know the puzzle's solution[9].

It remains to be seen whether this could compromise the identification process[10]. More-complicated schemes could defeat all possible quantum attacks[7,11], but they are currently beyond the reach of practical implementation. Further work is needed – both theoretical and technological – before these ideas can find their way to your local bank.

Gilles Brassard is in the Department of Computer Science and Operations Research, Université de Montréal, Montréal, Québec H3T 1J4, Canada.
e-mail: brassard@iro.umontreal.ca

1. Alikhani, P. *et al. Nature* **599**, 47–50 (2021).
2. Goldwasser, S., Micali, S. & Rackoff, C. *SIAM J. Comput.* **18**, 186–208 (1989).
3. Goldreich, O., Micali, S. & Wigderson, A. *J. Assoc. Comput. Mach.* **38**, 690–728 (1991).
4. Feige, U., Fiat, A. & Shamir, A. *J. Cryptol.* **1**, 77–94 (1988).
5. Shor, P. W. *SIAM J. Comput.* **26**, 1484–1509 (1997).
6. Ben-Or, M., Goldwasser, S., Kilian, J. & Wigderson, A. in *Proc. 20th Annu. ACM Symp. Theory of Computing* 113–131 (ACM, 1988).
7. Crépeau, C., Massenet, A., Salvail, L., Stinchcombe, L. S. & Yang, N. in *Proc. 1st Conf. Information-Theoretic Cryptography* 4:1–4:18 (LIPIcs, 2020).
8. Einstein, A., Podolsky, B. & Rosen, N. *Phys. Rev.* **47**, 777–780 (1935).
9. Bell, J. S. *Physics* **1**, 195–200 (1964).
10. Crépeau, C., Salvail, L., Simard, J.-R. & Tapp, A. in *Adv. Cryptol. — ASIACRYPT 2011* 407–430 (Springer, 2011).
11. Chailloux, A. & Leverrier, A. in *Adv. Cryptol. — EUROCRYPT 2017* Part III, 369–396 (Springer, 2017).

The author declares no competing interests.

Metabolism

A hormonal two-step to drive physical activity

Stephanie L. Padilla

In mice, the ovarian hormone oestradiol sensitizes neurons in a brain region called the hypothalamus to a melanocortin hormone that signals an energy surplus. Their dual activation increases physical activity. **See p.131**

Mammals become less physically active with ageing, and, in females, this decline in activity is tied to reproductive ageing. After menopause, women tend to be less active and to develop increased total fat mass and altered fat distribution[1]. In rodents, surgical removal of the ovaries (ovariectomy) reduces the levels of ovarian hormones such as oestradiol in a similar way to the effects of menopause, and results in reduced physical activity and corresponding increases in weight. On page 131, Krause *et al.*[2] identify a population of neurons in the ventrolateral subdivision of the brain's ventromedial hypothalamus (VMH) that are sensitive to oestradiol. These neurons regulate the balance between sedentary behaviour and physical activity on the basis of perceived energy state, with menopause and the associated reduction in oestradiol causing a shift towards sedentary behaviour.