The Economics of Retail Payment Security

Fumiko Hayashi[1] **Tyler Moore**[2] Richard J. Sullivan[1]

[1] Federal Reserve Bank of Kansas City
[2] Southern Methodist University, Dallas, TX
University of Tulsa, OK (from August 2015)
tyler-moore@utulsa.edu

The Puzzle of Payments Security
Federal Reserve Bank of Kansas City
June 25, 2015

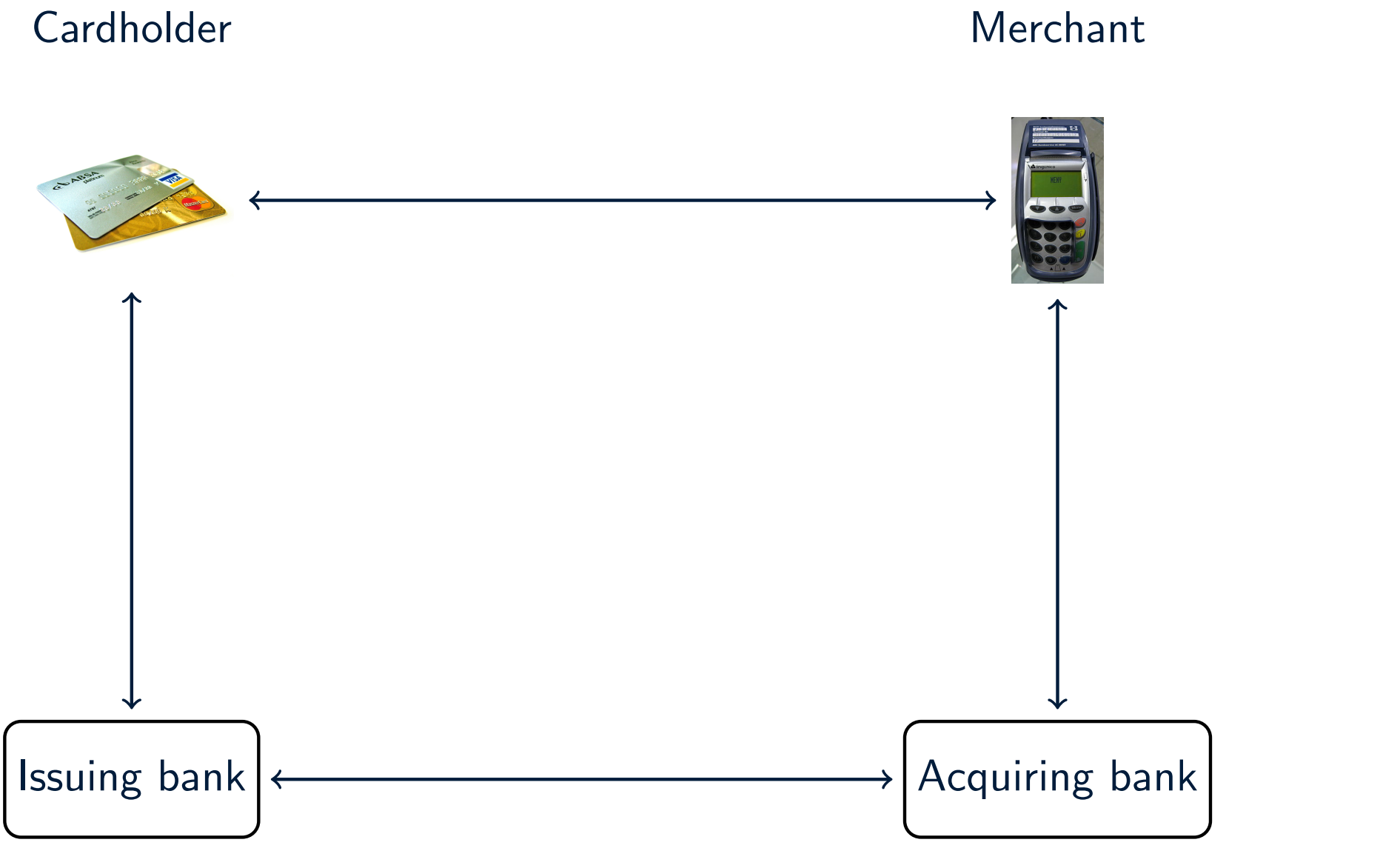
Motivation

- Payments system security is universally recognized as important
- Yet we continue to rely on less secure technologies
- Economics can help explain why, as well as offer guidance on how to improve security

Outline

Outline

Two-sided market structure



Network externalities, two-sided markets and security

- Positive network externalities on both sides (cardholders, merchants)
- Two-sided markets impose extensive barriers to entry
- This makes displacing successful ones, like payment-card networks, very difficult
- Hard for the dominant platform to justify investing in more secure technologies

Key principles affecting retail payments security

- Economies of scale and scope
  - Scale reduces cost per quantity, and multipurpose devices spread costs
  - Tends towards small number of large platforms that deter new entrants

Key principles affecting retail payments security

- Economies of scale and scope
  - Scale reduces cost per quantity, and multipurpose devices spread costs
  - Tends towards small number of large platforms that deter new entrants
- Jointly produced goods
  - Payment security depends on the efforts of many participants (e.g., merchant, merchant processor, acquirer, card network, issuer processor, and issuer all responsible to prevent data breaches)
  - Interdependency can lead to coordination failures

Key principles affecting retail payments security

- Economies of scale and scope
  - Scale reduces cost per quantity, and multipurpose devices spread costs
  - Tends towards small number of large platforms that deter new entrants
- Jointly produced goods
  - Payment security depends on the efforts of many participants (e.g., merchant, merchant processor, acquirer, card network, issuer processor, and issuer all responsible to prevent data breaches)
  - Interdependency can lead to coordination failures
- Competition *for* the market
  - Tension between backing proprietary security mechanisms (e.g., EMV) vs. open standards (e.g., AES)
  - Proprietary mechanisms offer clear incentive to backers, but open standards can attract wider adoption
  - Proprietary mechanisms are regularly found to be insecure due to hidden design

Misaligned incentives

- Systems often fail because people who could protect a system lack incentive to do so

Misaligned incentives

- Systems often fail because people who could protect a system lack incentive to do so
- Example: Retail banking in the 1990s
  - US banks have long been required to pay for ATM card fraud
  - In the UK, regulators favored banks, often made customer pay for fraud
  - Which country suffered more ATM fraud?

Misaligned incentives

- Systems often fail because people who could protect a system lack incentive to do so
- Example: Retail banking in the 1990s
  - US banks have long been required to pay for ATM card fraud
  - In the UK, regulators favored banks, often made customer pay for fraud
  - Which country suffered more ATM fraud? The UK

Misaligned incentives

- Systems often fail because people who could protect a system lack incentive to do so
- Example: Retail banking in the 1990s
  - US banks have long been required to pay for ATM card fraud
  - In the UK, regulators favored banks, often made customer pay for fraud
  - Which country suffered more ATM fraud? The UK
  - Since US banks had to pay for disputed transactions, banks had strong incentive to invest in technology to reduce fraud
  - Since UK banks could blame customers for fraud, they lacked incentive to invest in same anti-fraud mechanisms, hence the higher fraud

Markets with asymmetric information

Akerlof's market for lemons

- Suppose a town has 20 similar used cars for sale
  - 10 "cherries" valued at $2,000 each
  - 10 "lemons" valued at $1,000 each
  - What is the market-clearing price?

Akerlof's market for lemons

- Suppose a town has 20 similar used cars for sale
  - 10 "cherries" valued at $2,000 each
  - 10 "lemons" valued at $1,000 each
  - What is the market-clearing price?
- Answer: $1,000. Why?
  - Buyers cannot determine car quality, so they refuse to pay a premium for a high-quality car
  - Sellers know this, and only owners of lemons will sell for $1,000
  - The market is flooded with lemons (the bad drives out the good)

Information asymmetries in payments security

1. Secure software is a market for lemons
   - Vendors may believe their software is secure, but buyers have no reason to believe them
   - So buyers refuse to pay a premium for secure software, and vendors refuse to devote resources to do so

Information asymmetries in payments security

1. Secure software is a market for lemons
   - Vendors may believe their software is secure, but buyers have no reason to believe them
   - So buyers refuse to pay a premium for secure software, and vendors refuse to devote resources to do so
2. Lack of robust incident data on fraud and attacks
   - Banks and merchants may not want to reveal fraud losses for fear it will scare away customers, embolden regulators or attract lawsuits
   - But this makes it hard to understand the true magnitude of risks or efficiently allocate defensive resources

Consequences of asymmetric information

1. Adverse selection
   - Low-quality more likely to participate than high-quality in efforts that cannot assess quality
   - Insecure payment terminals more likely to seek (and receive) security certifications than secure ones
2. Moral hazard
   - Engaging in risky behavior because one is protected from its consequences
   - Sometimes claimed that consumers engage in moral hazard due to $0 card fraud liability
   - Cuts both ways: if regulations favor banks, they may behave recklessly in combating fraud

Outline

Game theory and the challenge of interdependent security

- Game theory is the formal study of conflict and cooperation
- Can be applied whenever outcomes depend on actions taken by others
- Improvements to retail payments security often require the cooperation of stakeholders with different interests

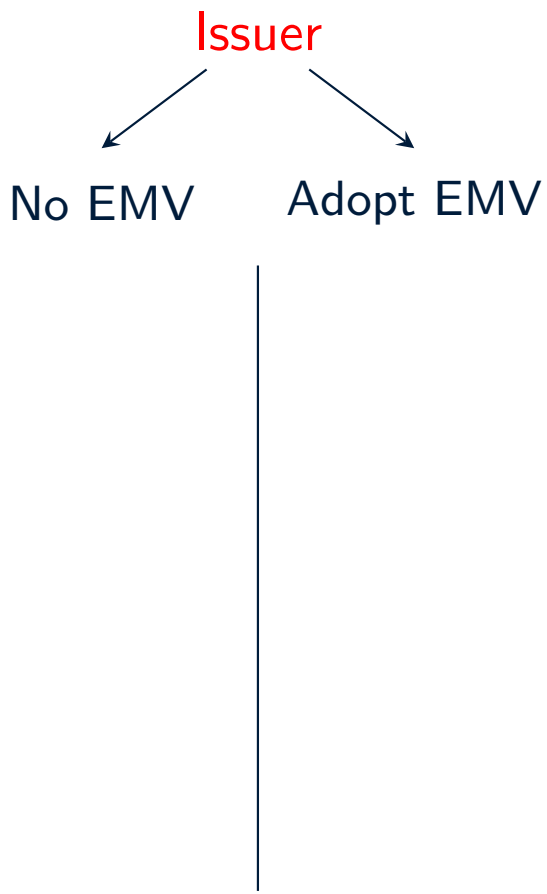
Game theory

- Game theory is a useful tool for predicting the most likely outcomes and identifying sources of conflict, if any
- Game theory can also inform policymakers and payments operators about how to shift behavior towards more desirable outcomes
- We illustrate its power with a topical example: EMV adoption

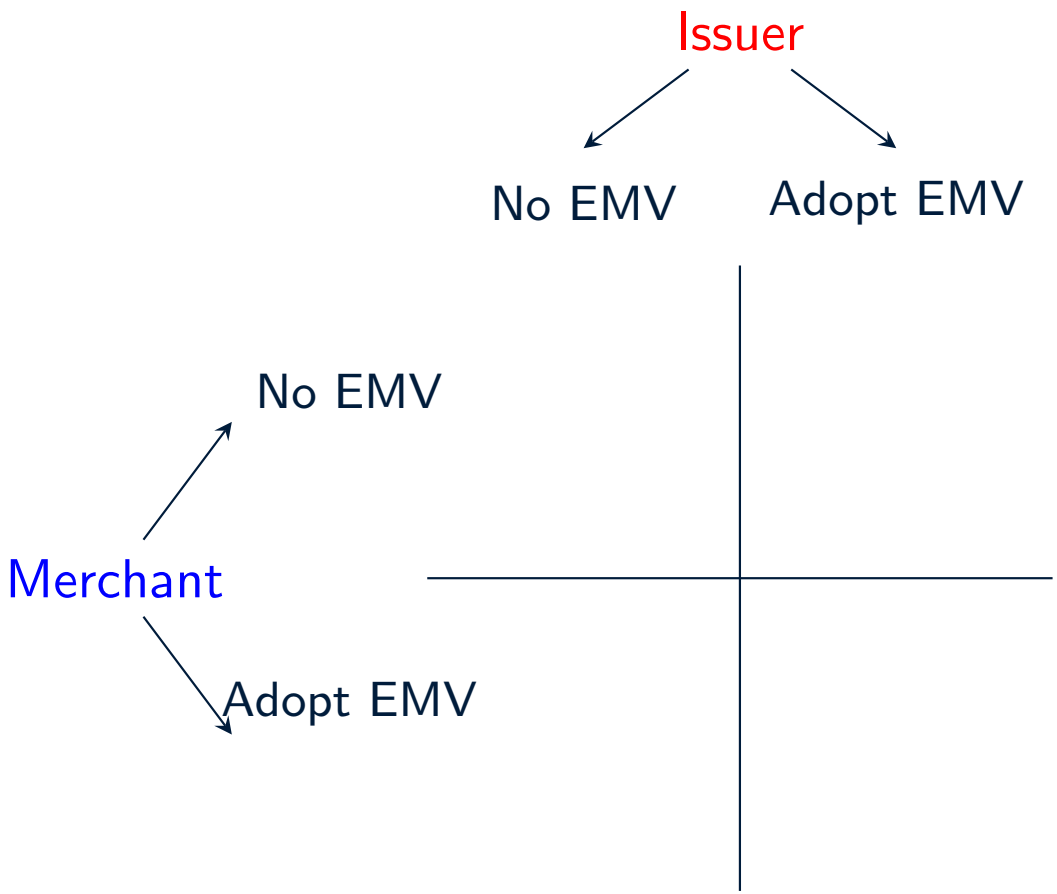
Game for EMV adoption in US

- Two players: issuer vs. merchant
- Two possible actions for both players: No EMV (status quo) vs. Adopt EMV
- Adopting EMV costs 2 for each player
- Currently card-present fraud liability is on issuers
- If both adopt EMV, issuer can reduce fraud loss by 4

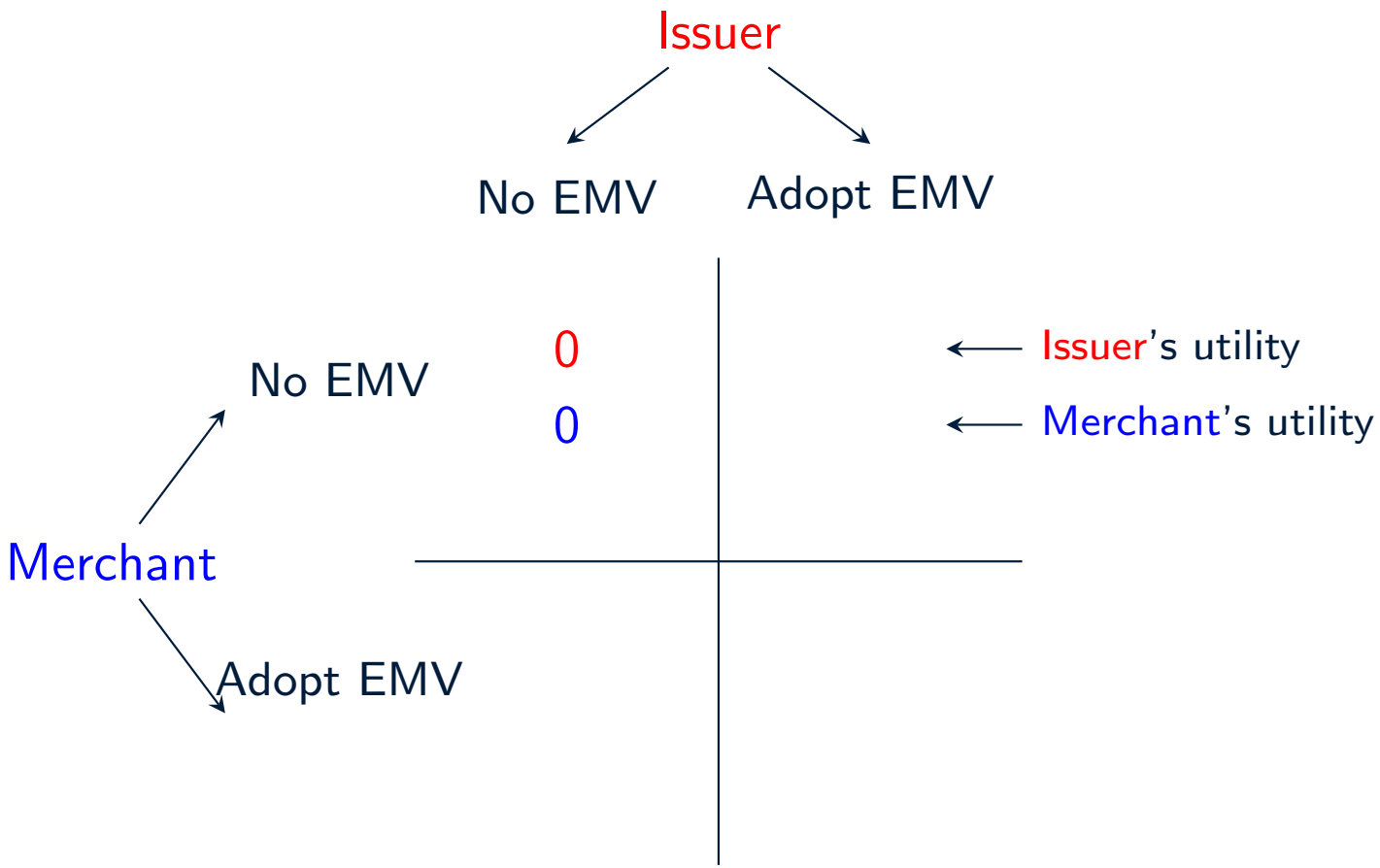
Game for EMV Adoption in US



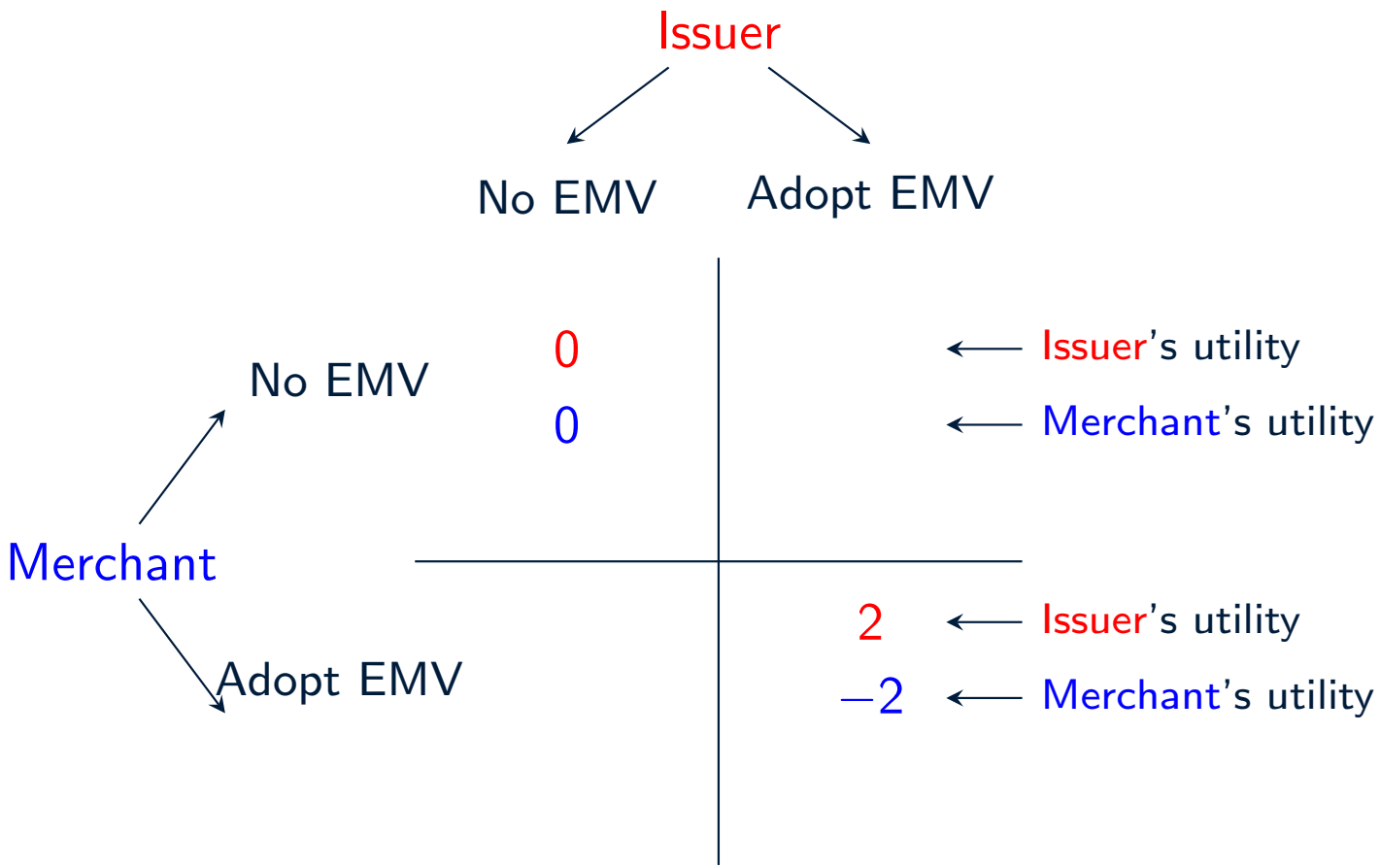
Game for EMV Adoption in US



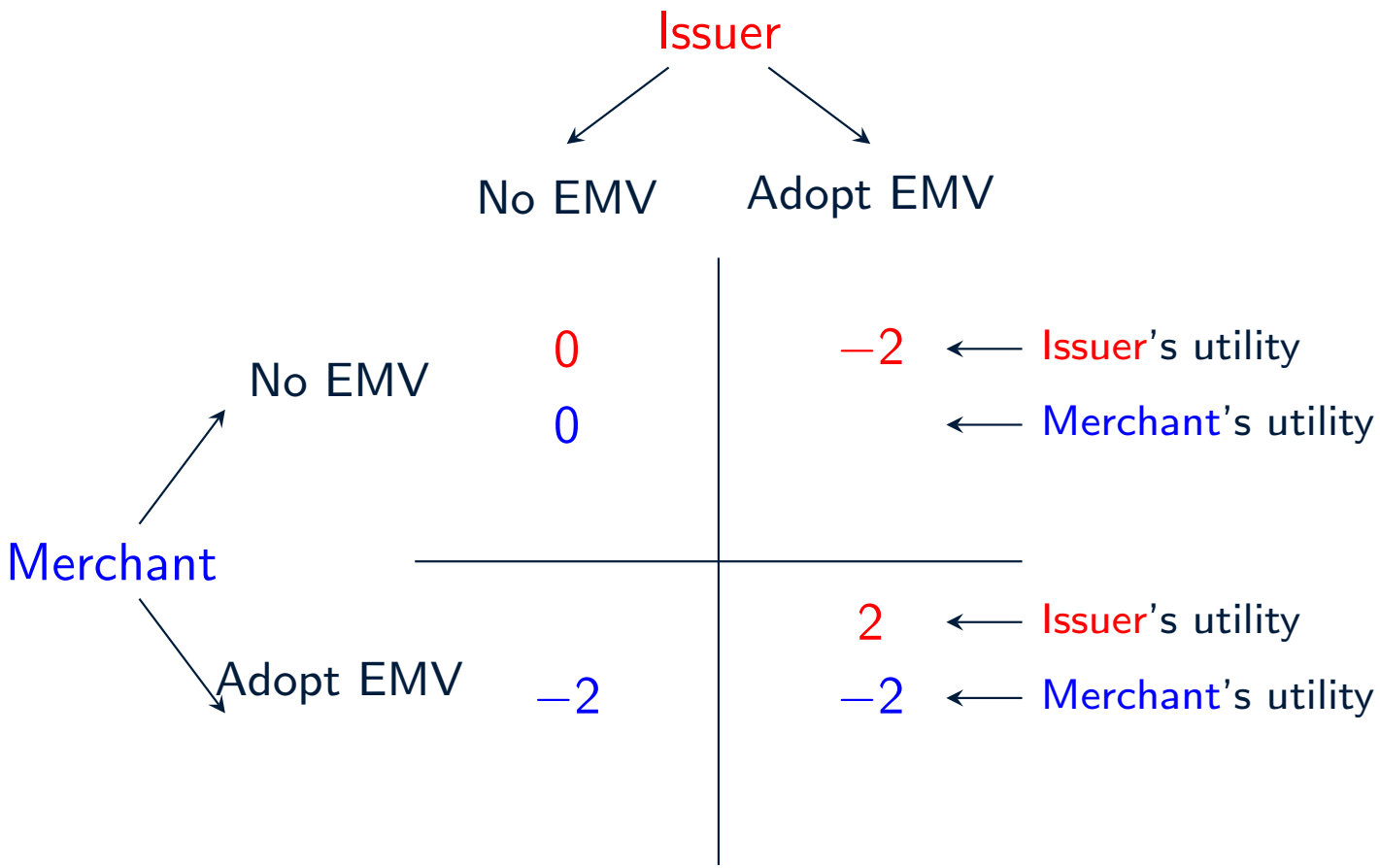
Game for EMV Adoption in US



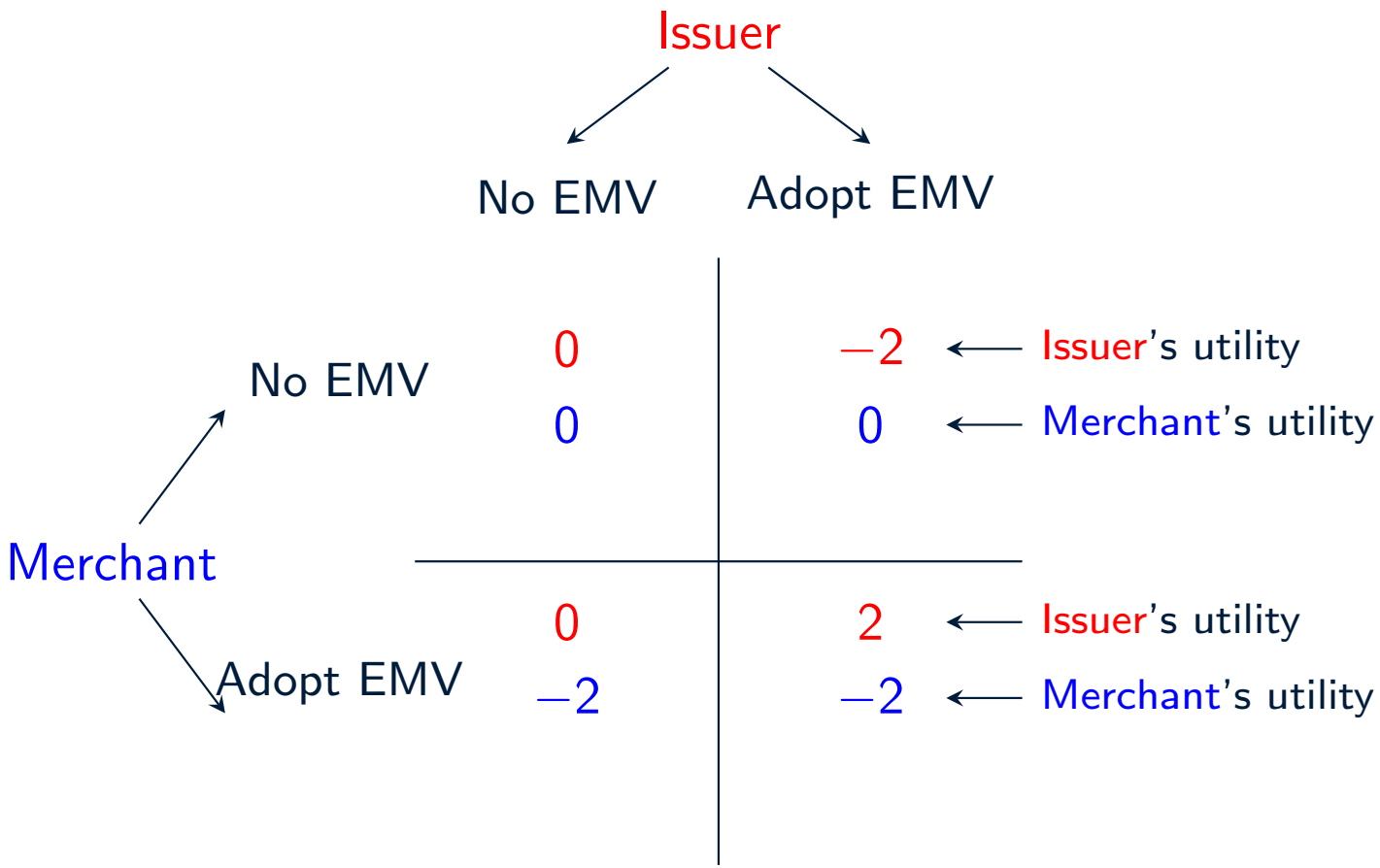
Game for EMV Adoption in US



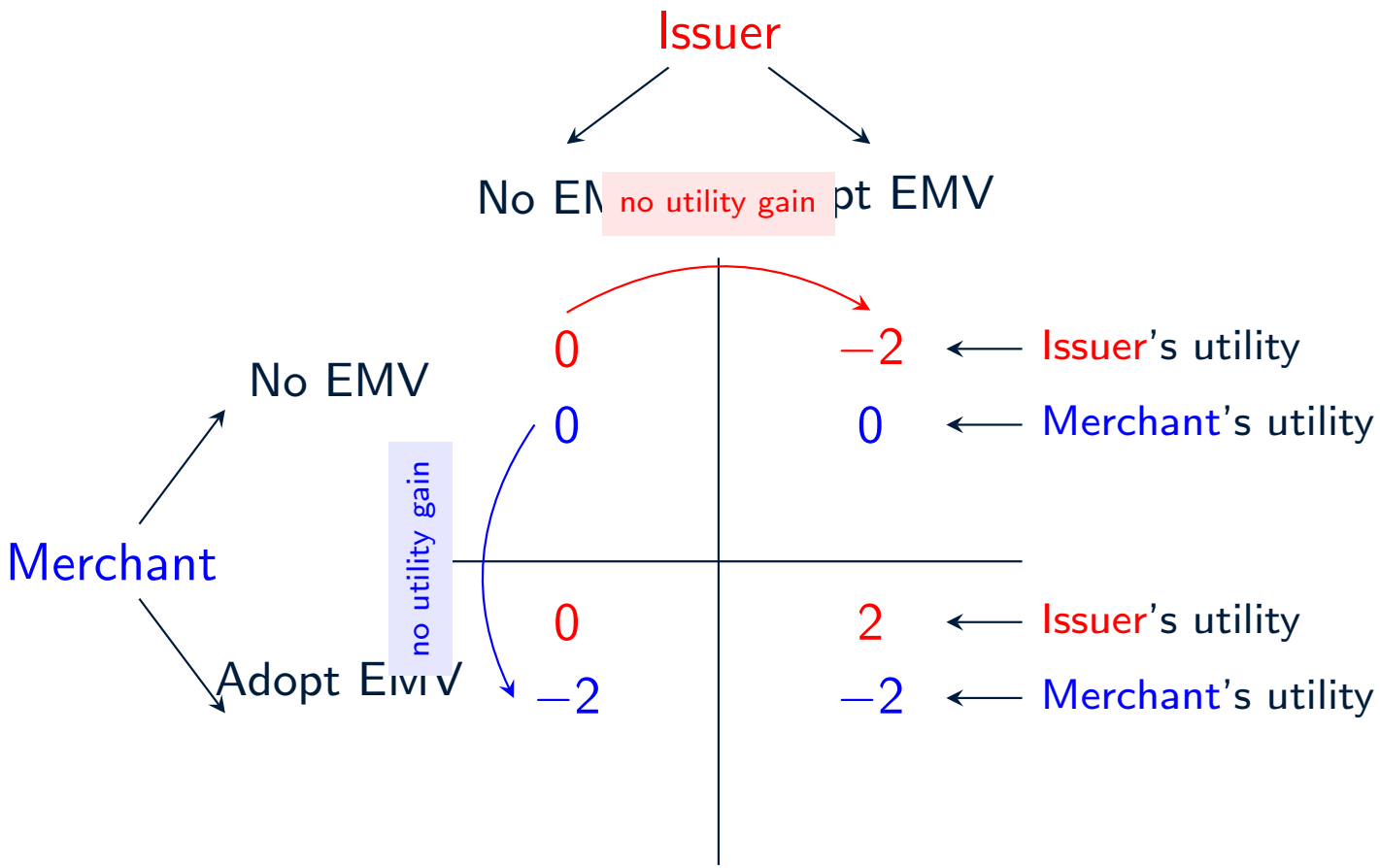
Game for EMV Adoption in US



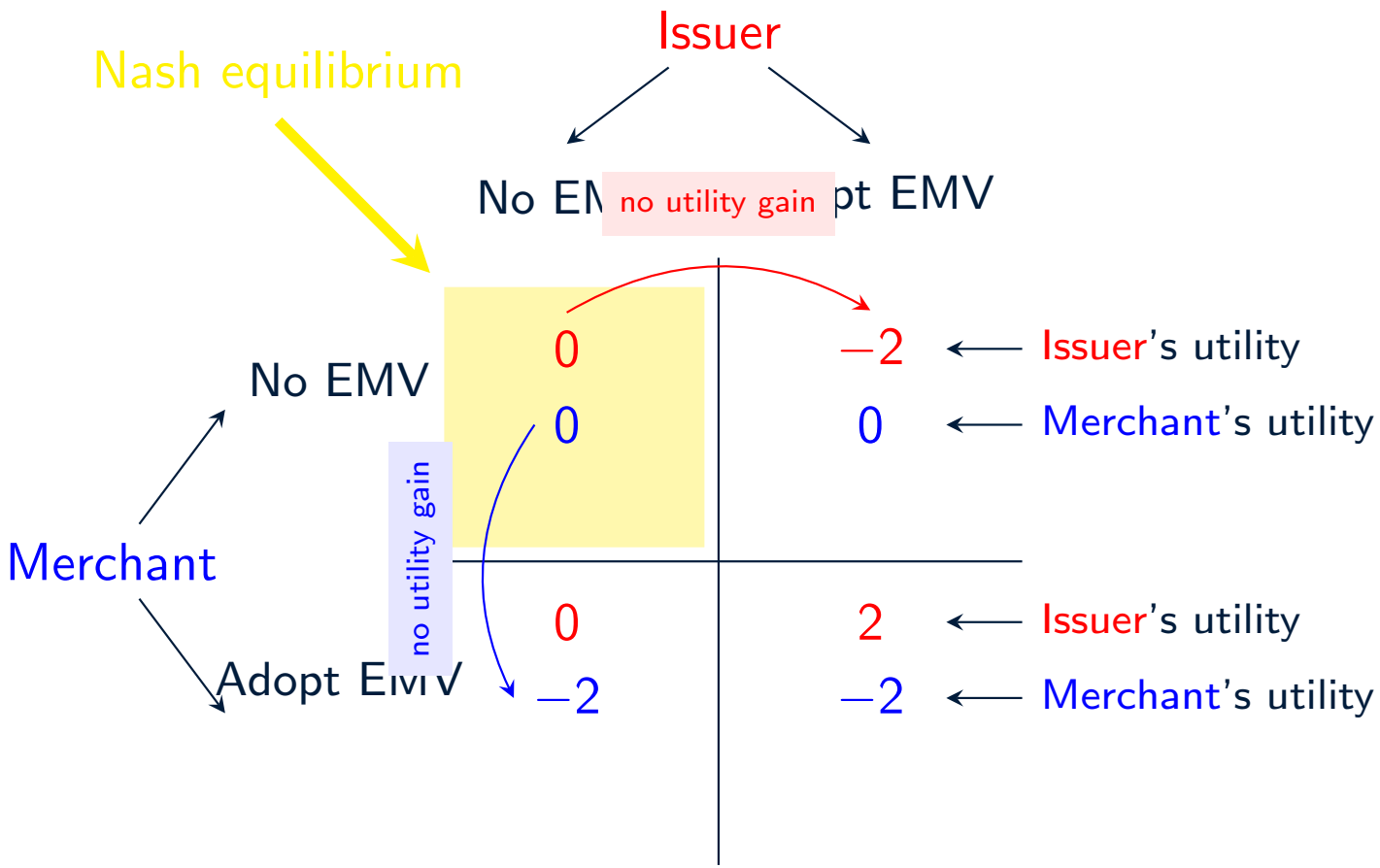
Game for EMV Adoption in US



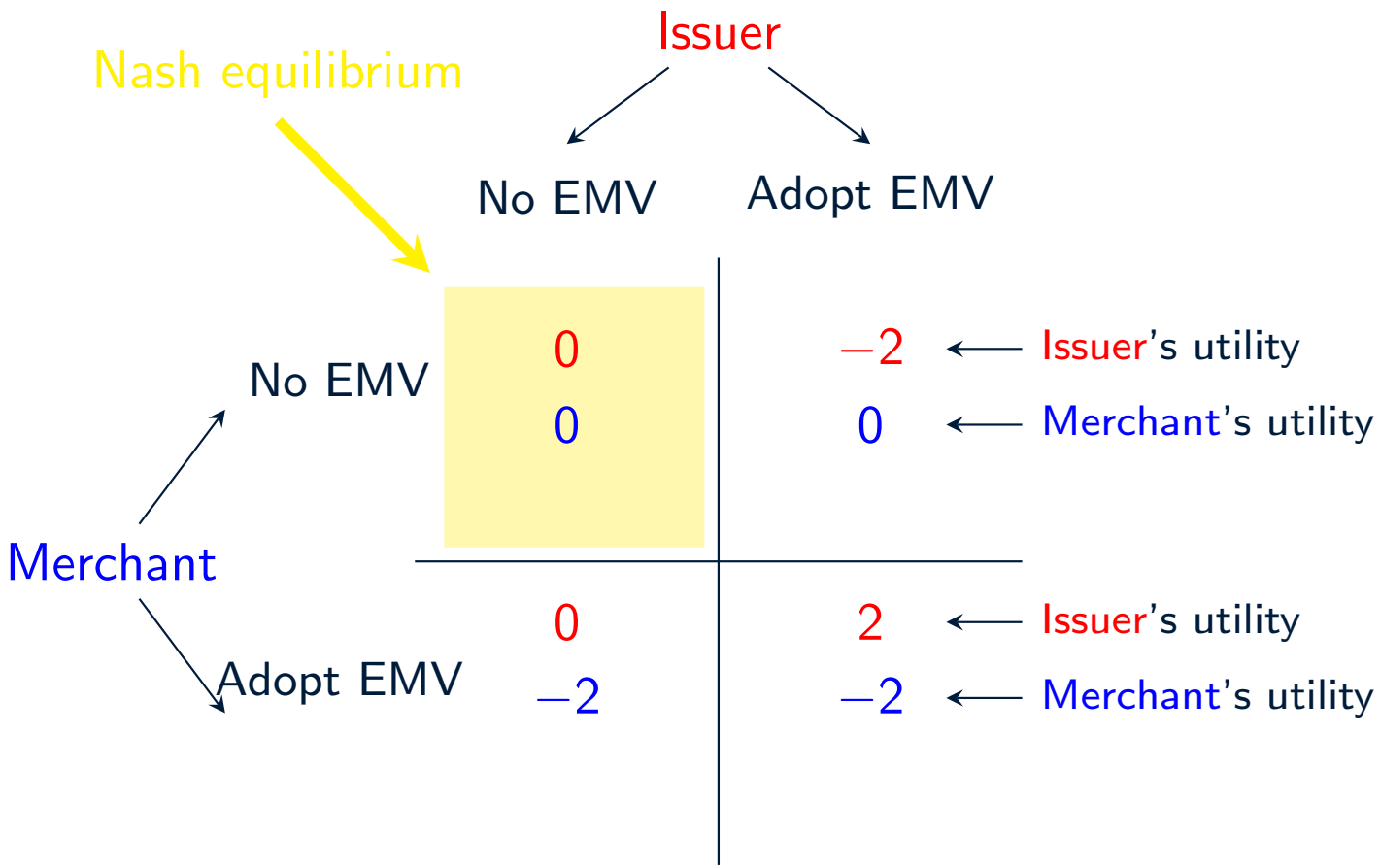
Game for EMV Adoption in US



Game for EMV Adoption in US



Game for EMV Adoption in US

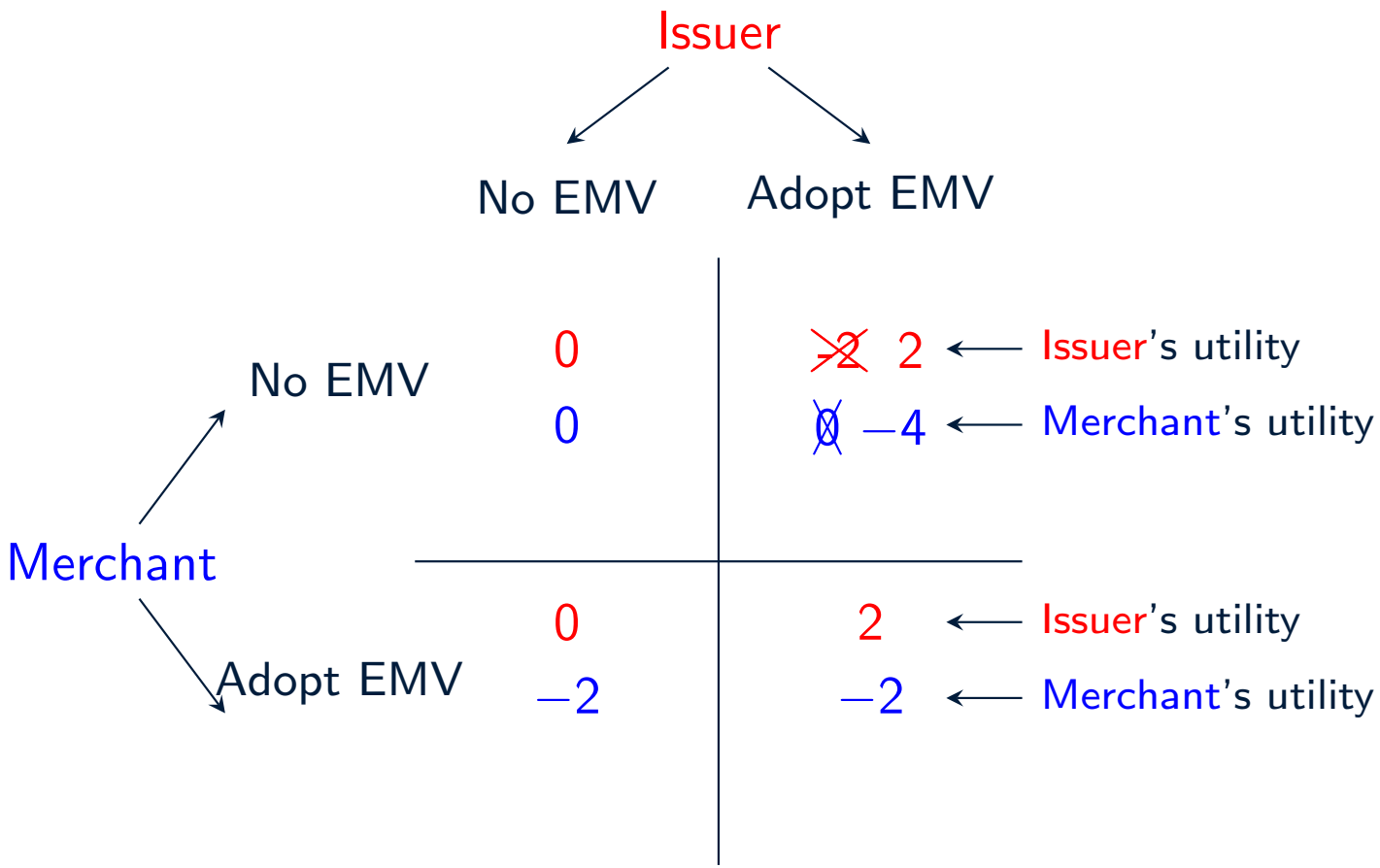


→ **Under current liability rules, equilibrium is to not upgrade**

Game for EMV Adoption in US

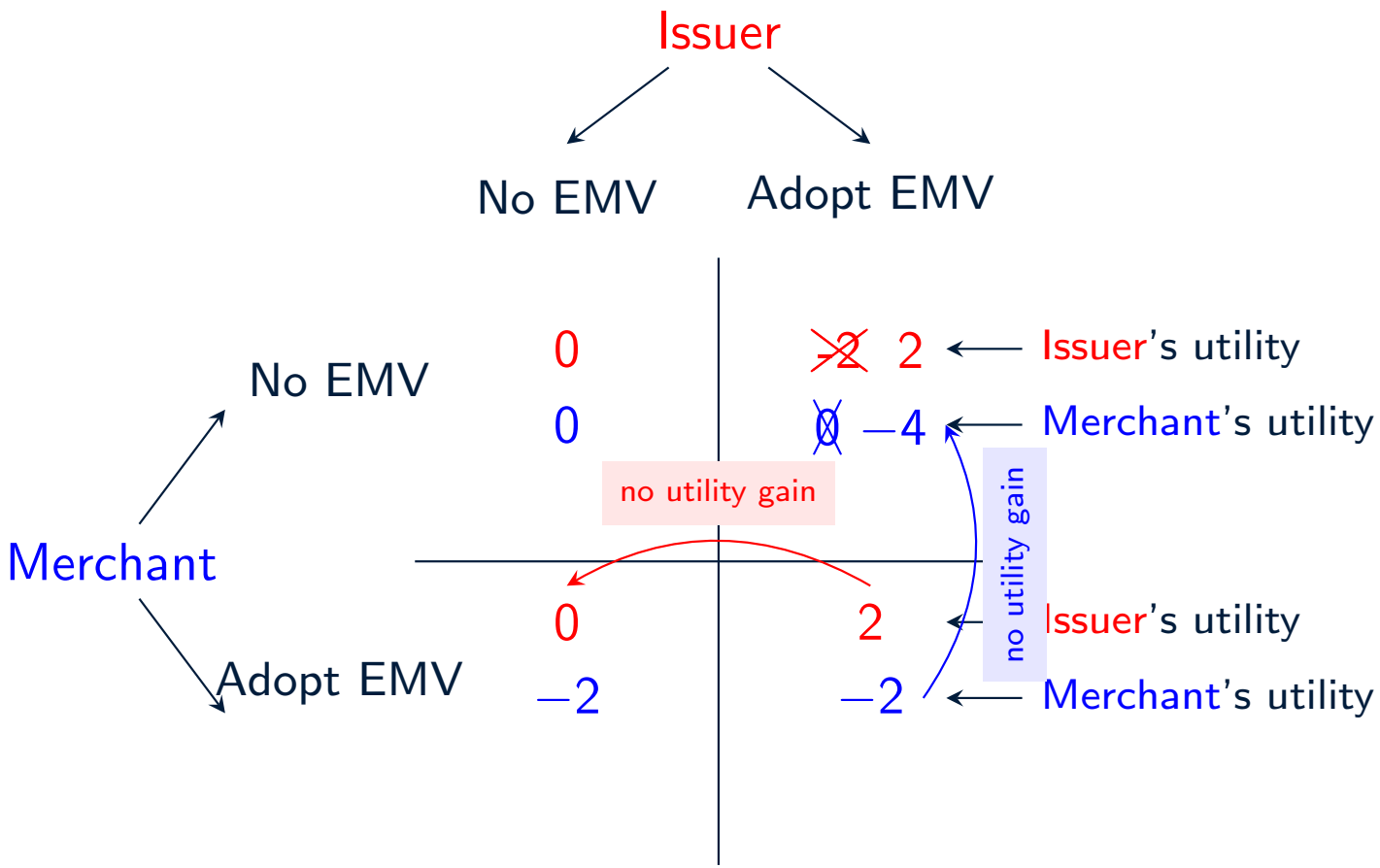
What will happen under new liability rules where the liability shifts to a merchant if the merchant does not upgrade but the issuer does?

Game for EMV Adoption in US



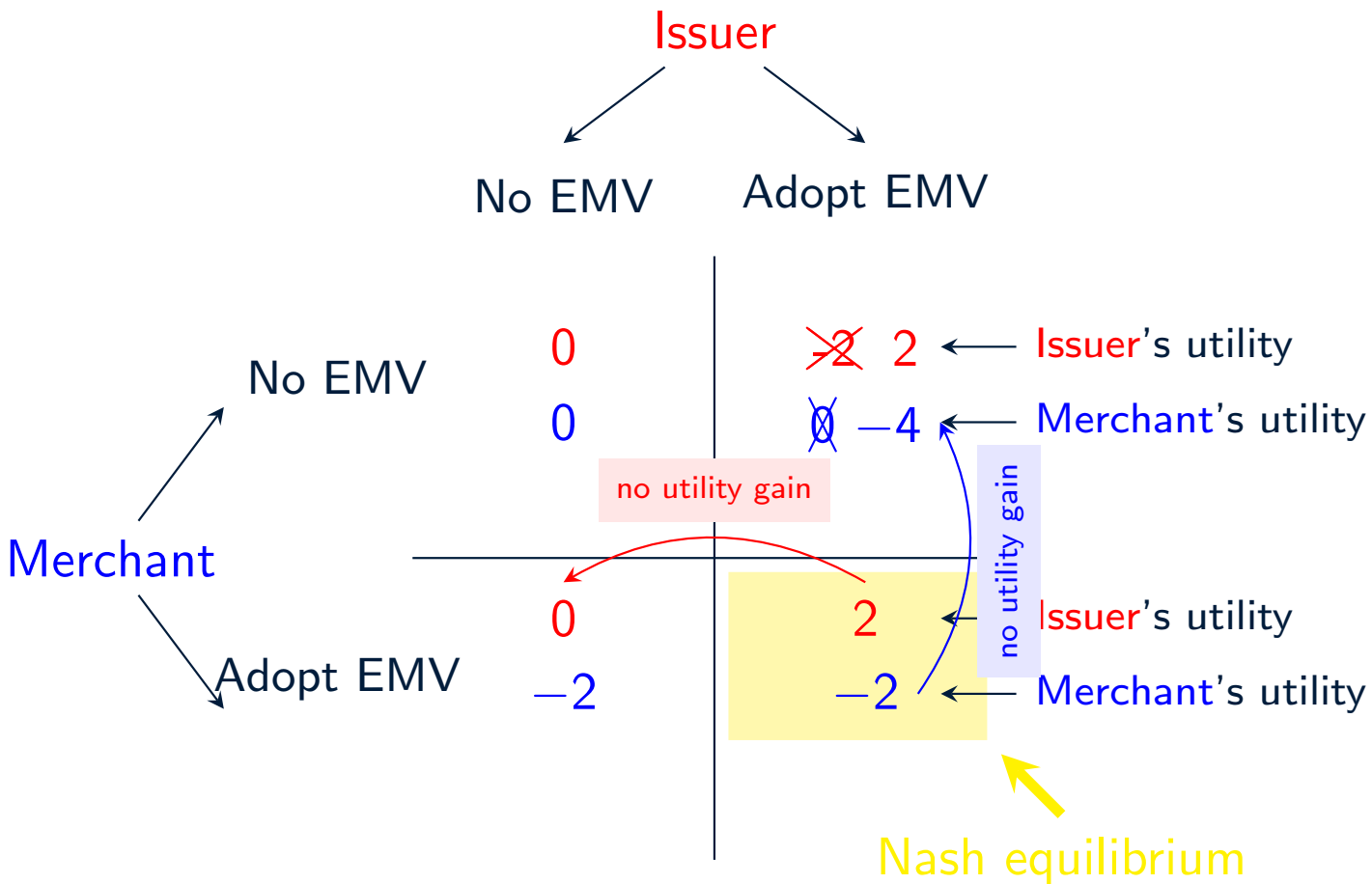
What will happen under new liability rules where the liability shifts to a merchant if the merchant does not upgrade but the issuer does?

Game for EMV Adoption in US



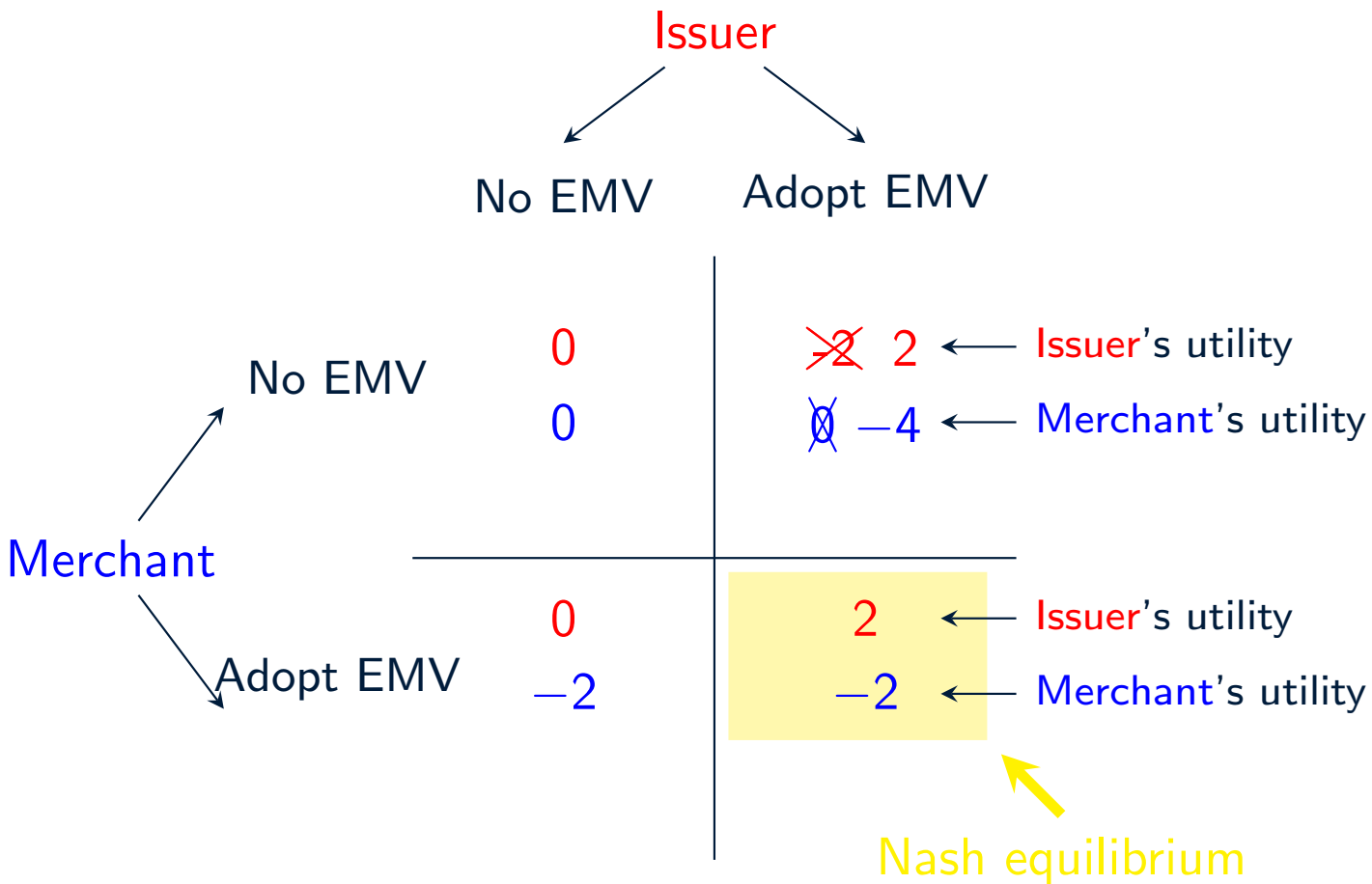
What will happen under new liability rules where the liability shifts to a merchant if the merchant does not upgrade but the issuer does?

Game for EMV Adoption in US



What will happen under new liability rules where the liability shifts to a merchant if the merchant does not upgrade but the issuer does?

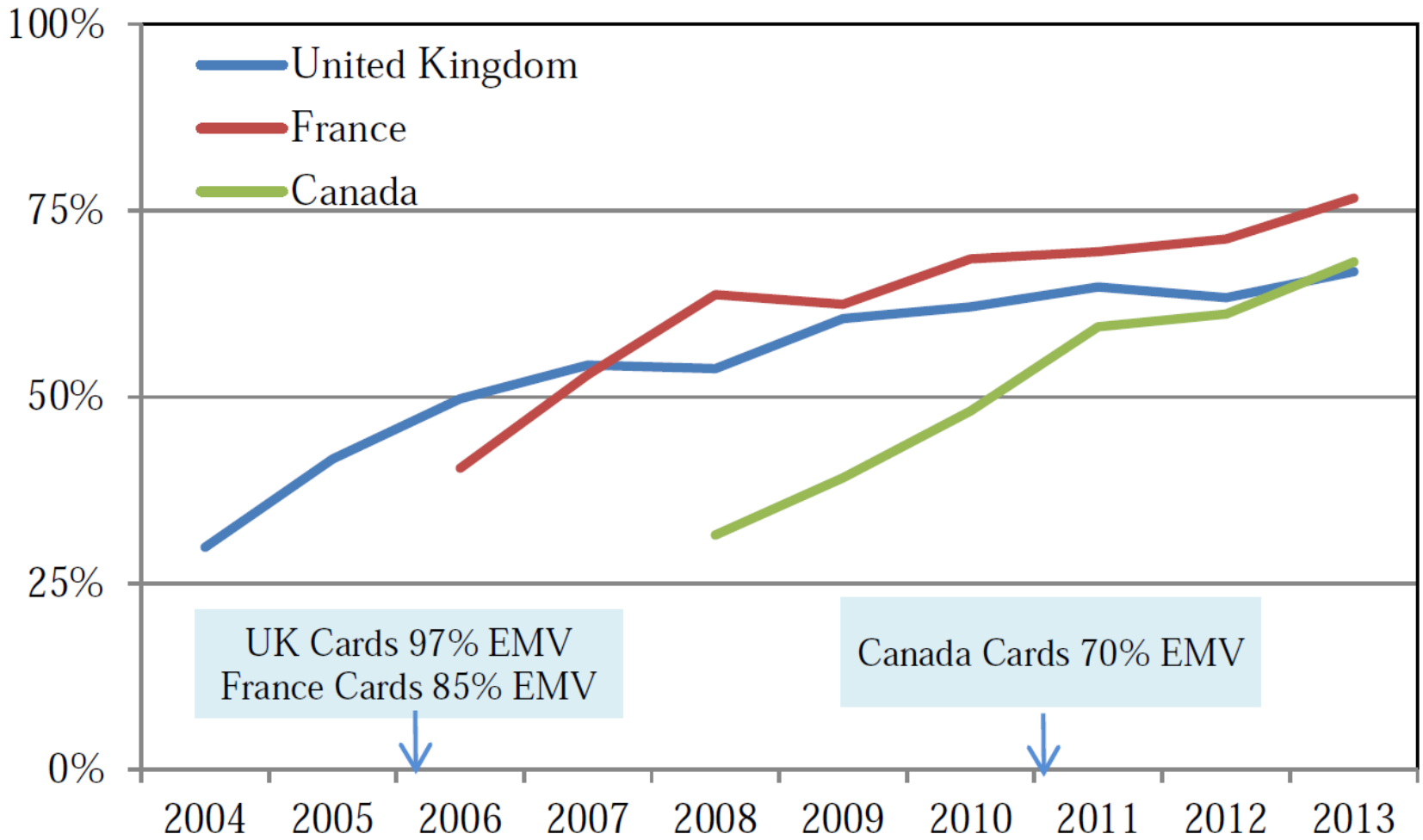
Game for EMV Adoption in US



→ **Under new liability rules, equilibrium is to upgrade**

Outline

CNP fraud share of total fraud rises following EMV adoption



Sources: Financial Fraud Action; Canadian Bankers Association, Credit Card Fraud Statistics; OPCS; Lucas (2011).

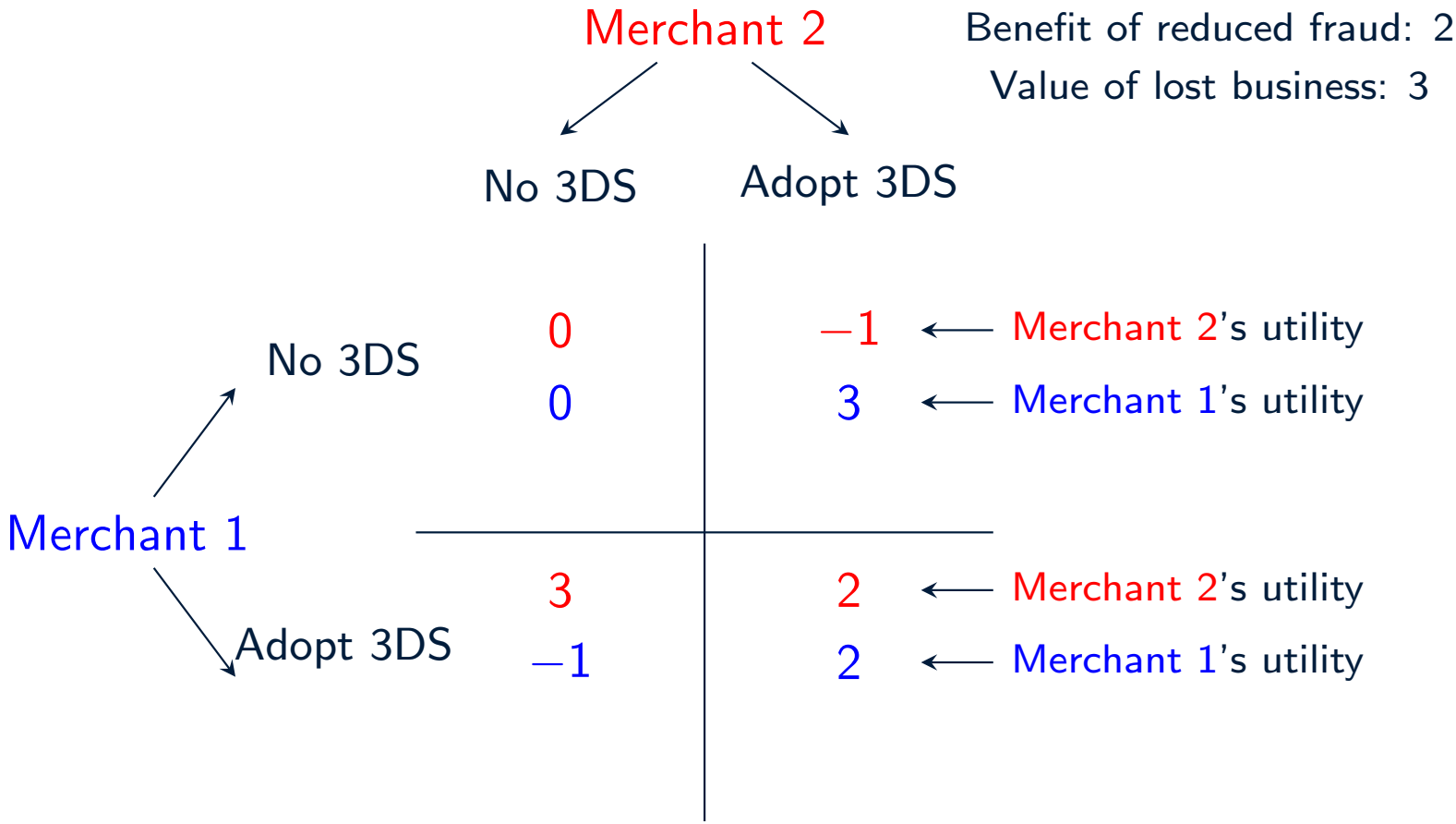
Improving authentication for online purchases

- Improved authentication systems are available for online purchases
  - SMS verification for logins
  - 3DSecure: password-augmented authentication proposed by Visa and MasterCard
- But merchants, issuers, and consumers lack incentive to adopt

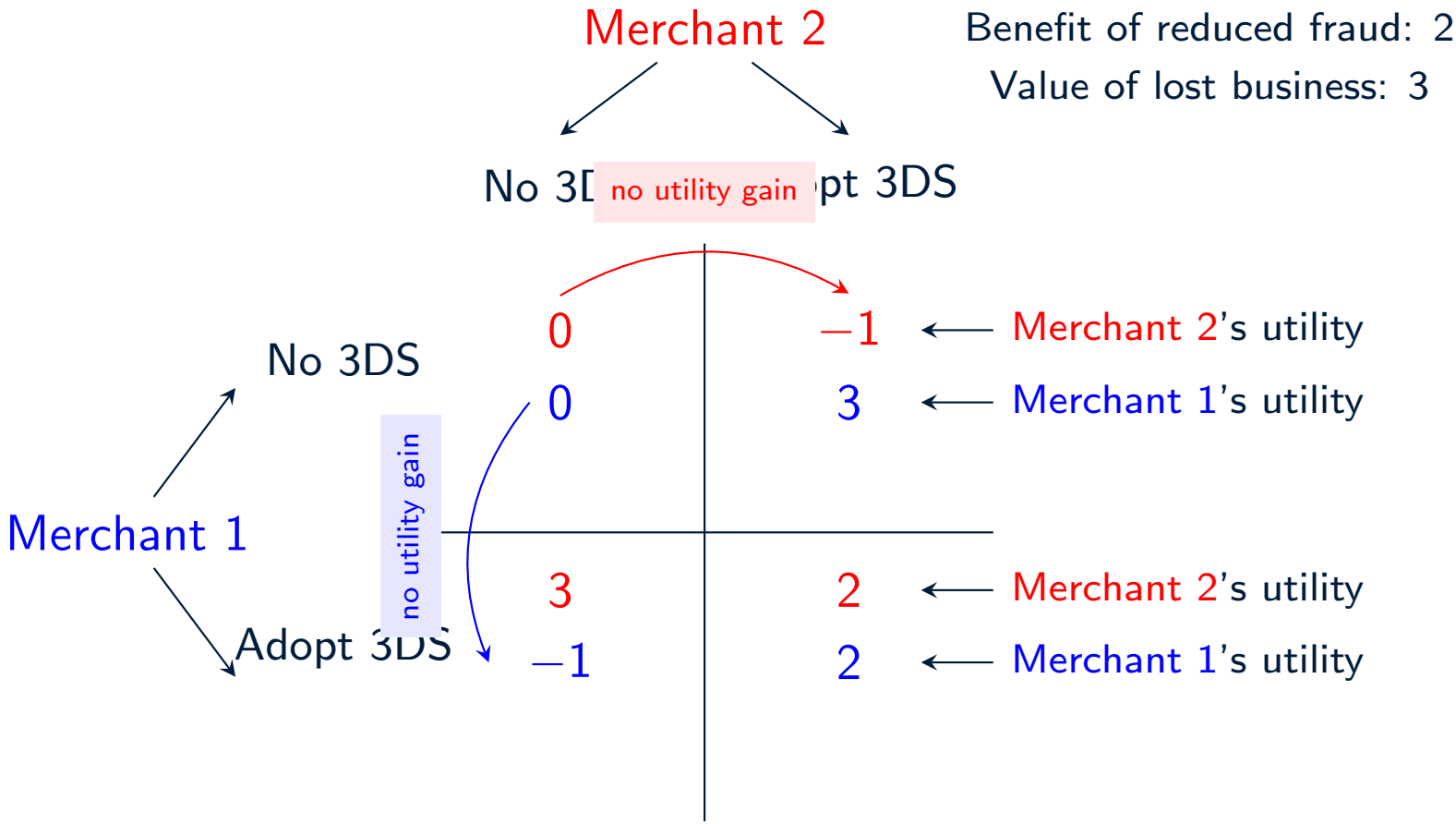
Improving authentication for online purchases

- Improved authentication systems are available for online purchases
  - SMS verification for logins
  - 3DSecure: password-augmented authentication proposed by Visa and MasterCard
- But merchants, issuers, and consumers lack incentive to adopt
- Game for 3DSecure in US
  - Two players: merchant vs. merchant, with CNP fraud liability
  - Two possible actions: No 3DS (status quo) vs. Adopt 3DS
  - Adopting 3DS costs 2 for each player
  - Adopting 3DS reduces fraud, but lose business if other merchants don't

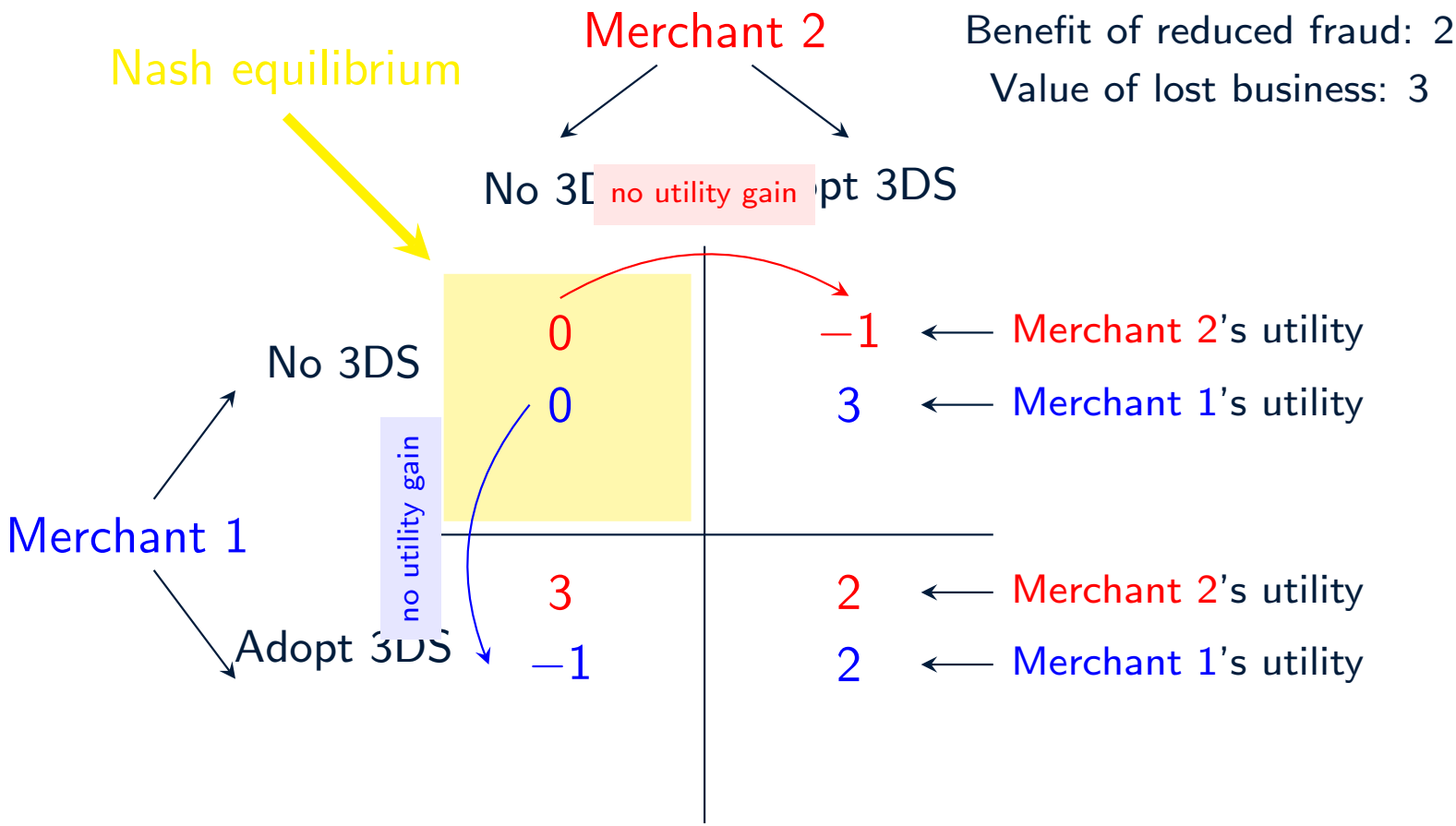
Game for 3DSecure Adoption in US



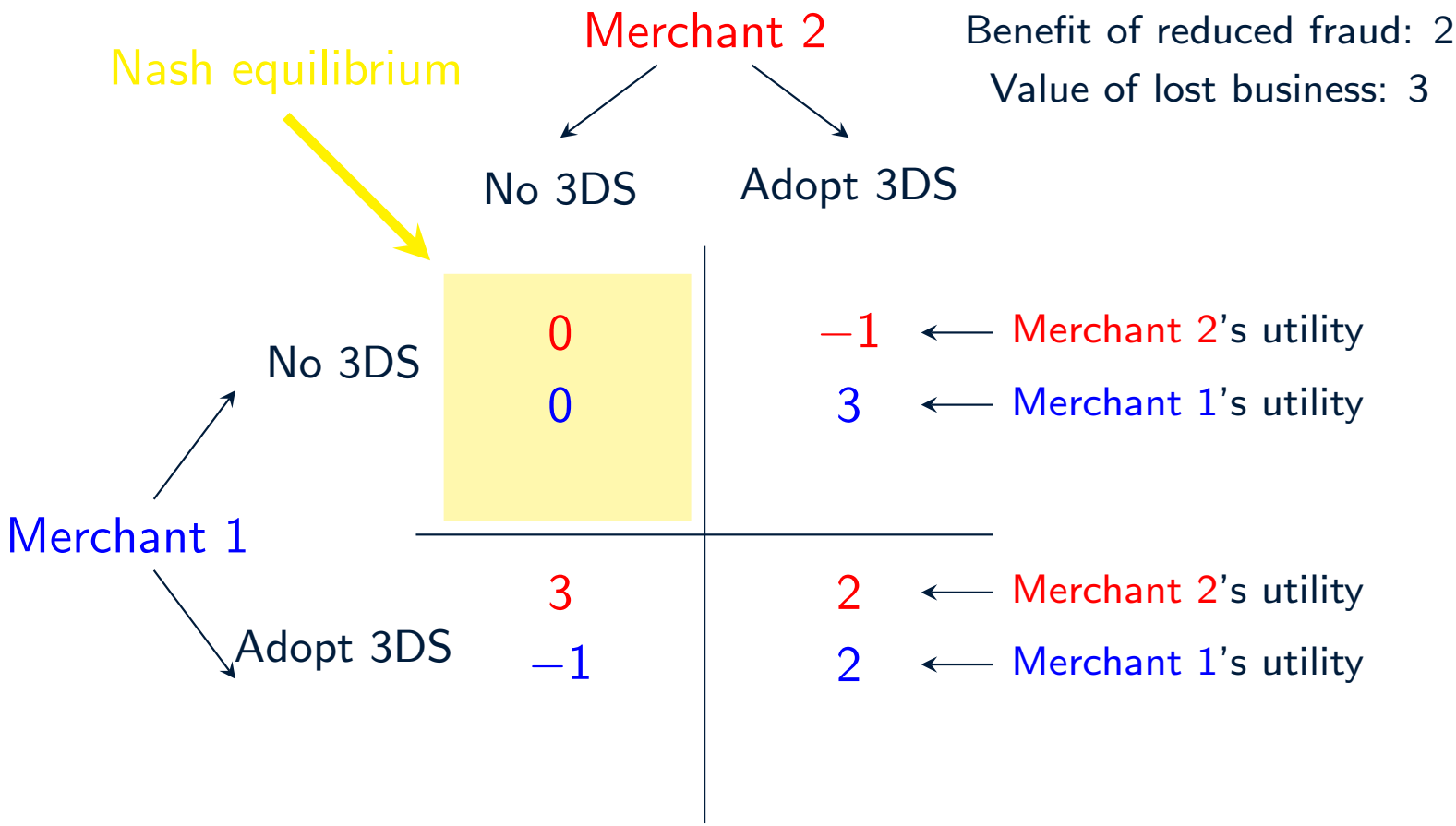
Game for 3DSecure Adoption in US



Game for 3DSecure Adoption in US



Game for 3DSecure Adoption in US

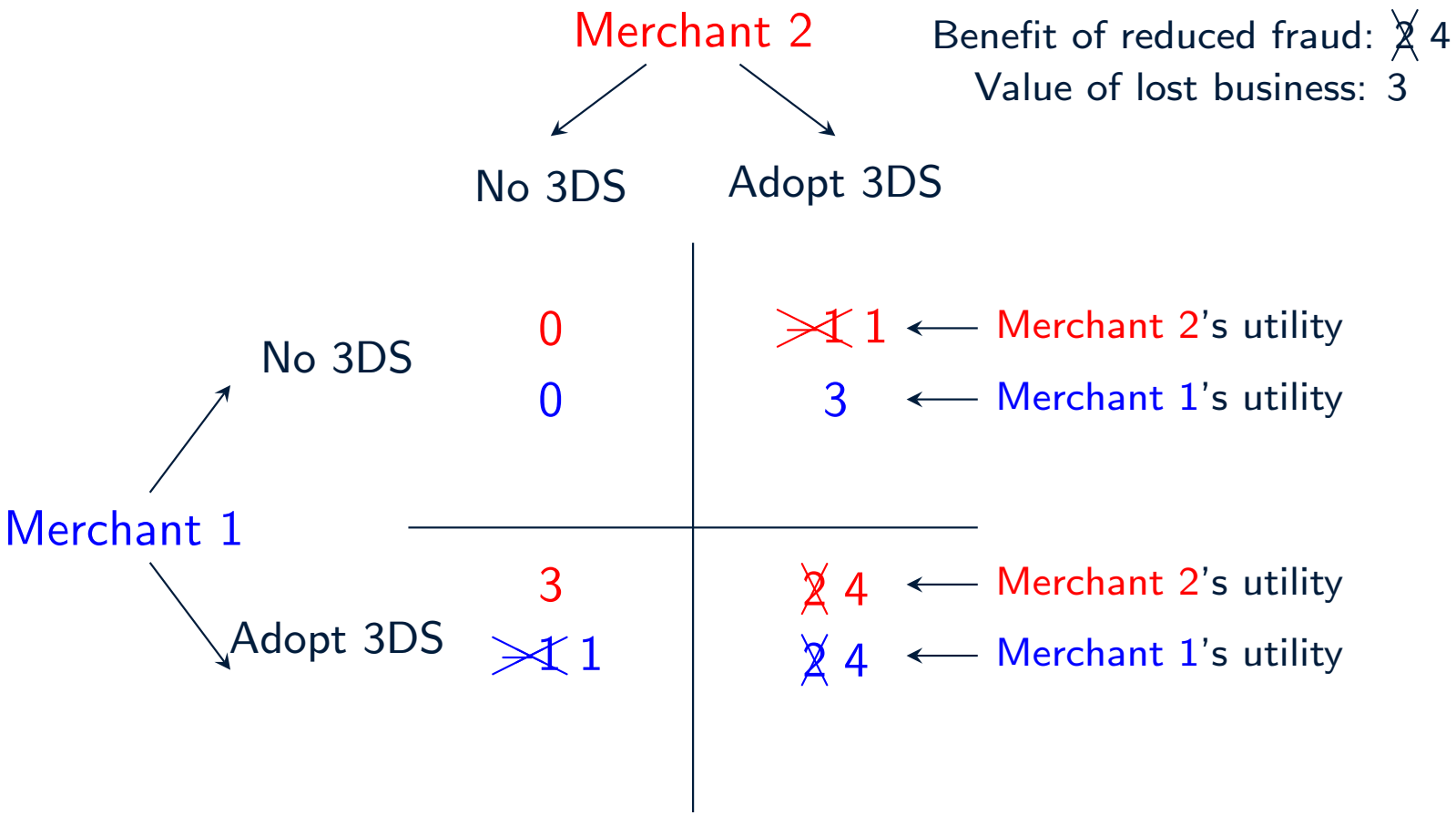


With low issuer participation or no liability shift, no adoption

Game for 3DSecure Adoption in US

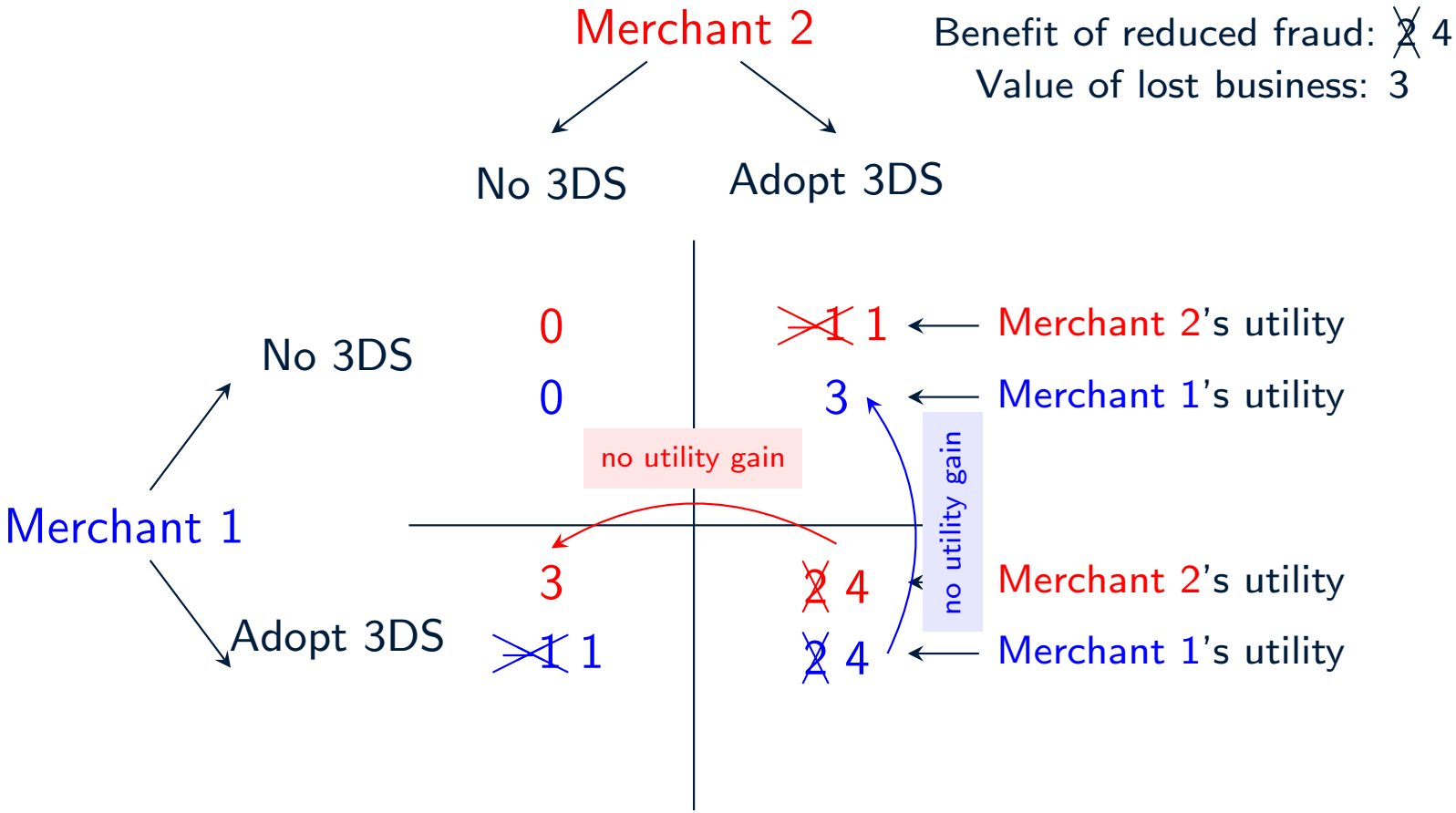
What if fraud losses for merchants are reduced by liability shift and increased issuer adoption?

Game for 3DSecure Adoption in US



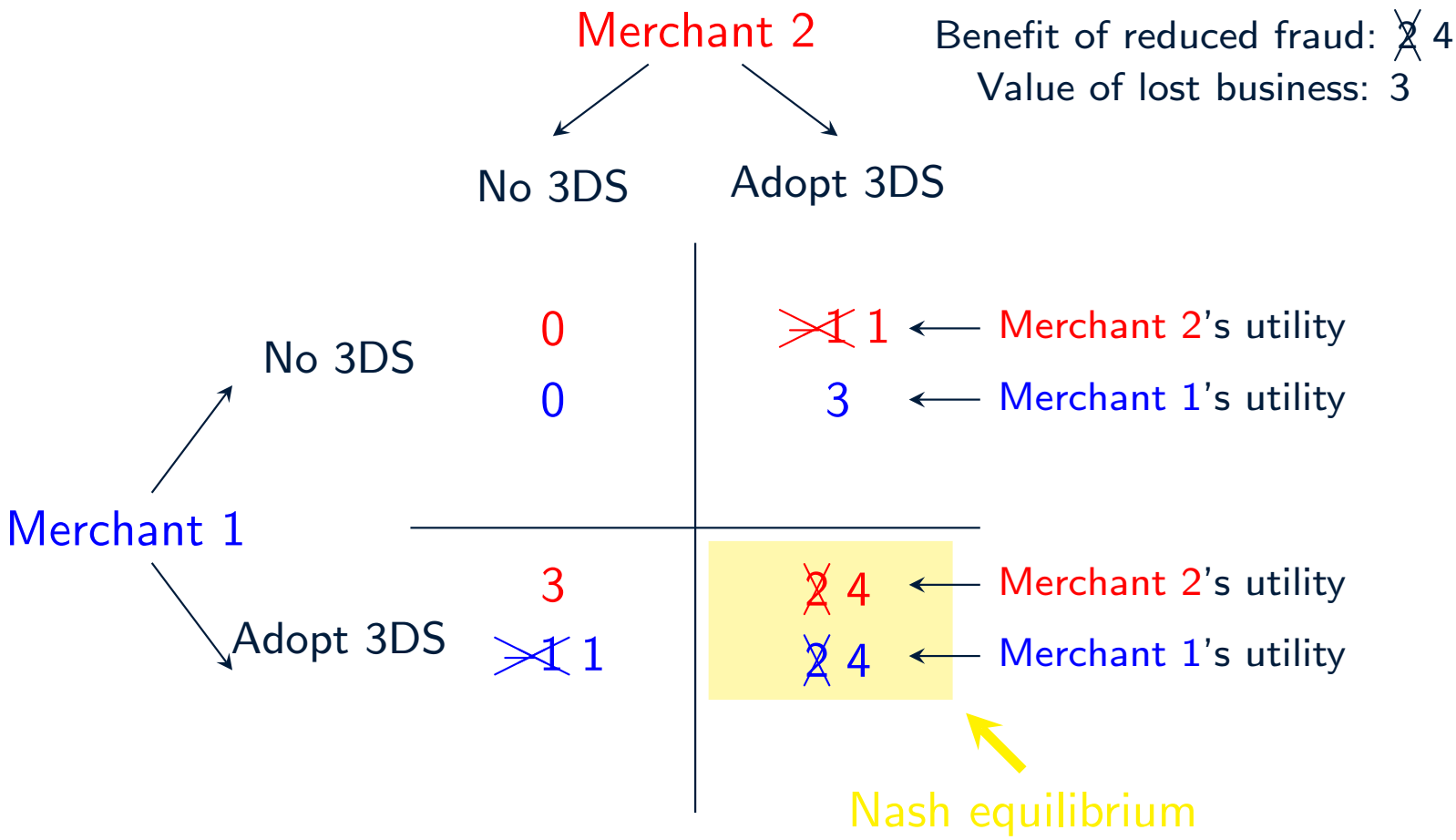
What if fraud losses for merchants are reduced by liability shift and increased issuer adoption?

Game for 3DSecure Adoption in US



What if fraud losses for merchants are reduced by liability shift and increased issuer adoption?

Game for 3DSecure Adoption in US

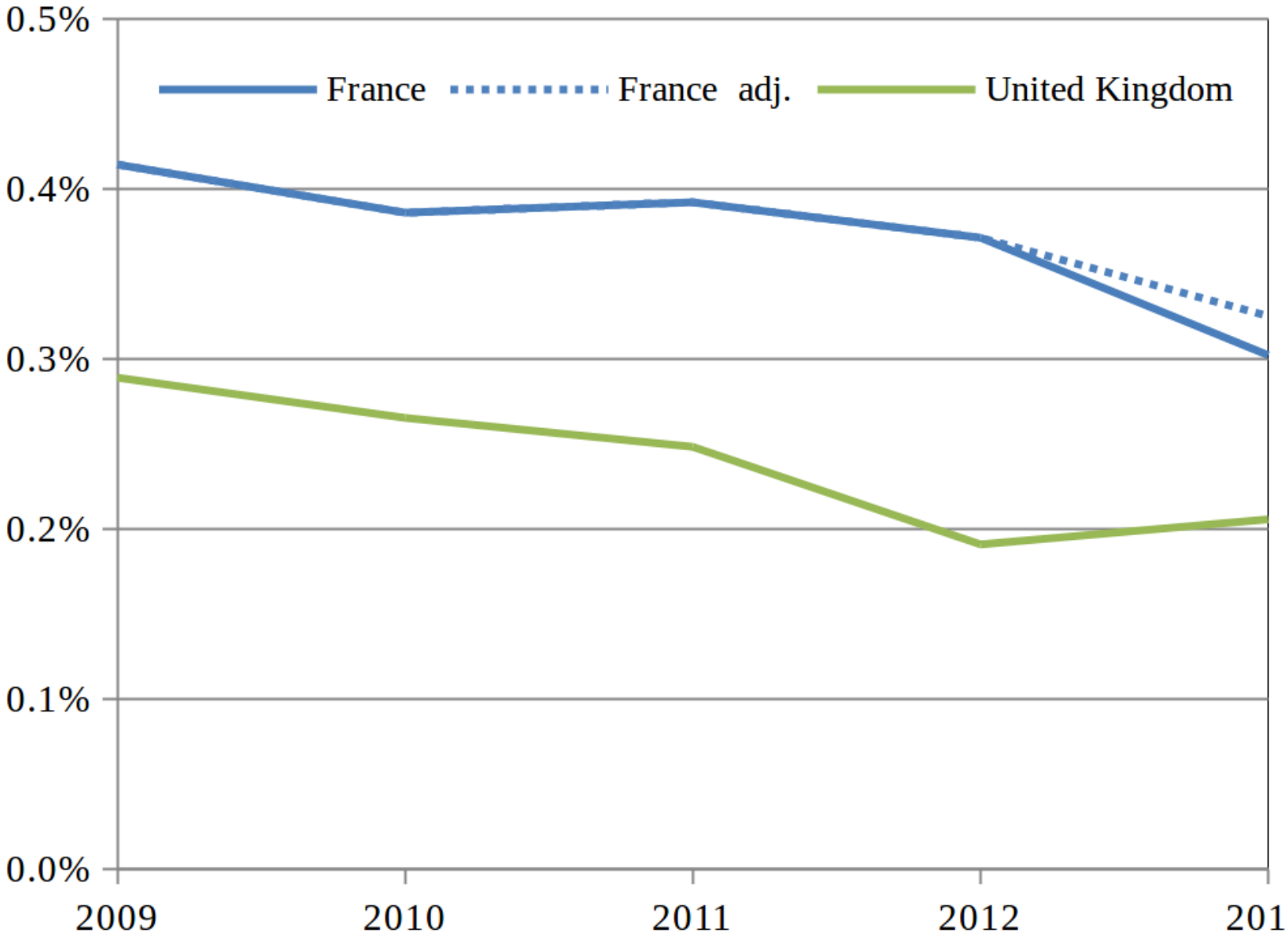


When reduced fraud exceeds lost business, equilibrium is to upgrade

Lessons from other countries' 3DSecure adoption

- France: central-bank led effort
  - Bank of France started by publishing data on high CNP fraud rates
  - Investigated technologies, but did not prescribe 3DSecure
  - Consulted with consumers, merchants and issuers but let them decide which defense to adopt
- UK: stakeholder-led effort
  - Immediate focus was on adopting 3DSecure
  - Acquirers gave merchants incentives to adopt
  - Addressed cart abandonment concern by limiting use to high-risk transactions

Fraud loss rate for internet transactions



The failure of PCI compliance to ward off data breaches

- Data breaches pose huge threat, both in terms of payment fraud and especially reputational risk
- The Payment Card System Data Security Standard (PCI DSS) is a self-regulatory approach designed to improve operational security of merchants
- 97% of Level 1 ($>$ 6M annual transactions) and 88% of Level 2 (1–6M annual transactions) U.S. merchants are PCI compliant

The failure of PCI compliance to ward off data breaches

- Data breaches pose huge threat, both in terms of payment fraud and especially reputational risk
- The Payment Card System Data Security Standard (PCI DSS) is a self-regulatory approach designed to improve operational security of merchants
- 97% of Level 1 ($>$ 6M annual transactions) and 88% of Level 2 (1–6M annual transactions) U.S. merchants are PCI compliant
- Yet data breaches remain pervasive
  - Interdependent security from jointly produced goods is hard to achieve
  - Misaligned incentives also play a big role

Misaligned incentives to protect card data

- Card brands and issuers value security but may prefer convenience in the payment process to enhanced security
- Merchant acquirers often specify in contracts that merchants are responsible for fines arising from PCI non-compliance, which dulls incentive to monitor clients
- Merchants spend heavily to implement PCI DSS but are frequently found to be out of compliance following a breach and held liable
- The prospect for retroactive non-compliance dulls the incentive to become compliant in the first place or take more than minimum effort
- Uncertainty over when a breach might occur and who pays can dull the incentive for all parties to take adequate precautions

Mobile payment platform overview

- New entrants waging battle to establish dominant platforms
  - Google Wallet aka Android Pay: NFC with cloud-based tokenization
  - Apple Pay: NFC with local tokenization
  - CurrentC: QR-code system tied to bank accounts
- All platforms more secure than existing approaches, but each benefits its backer's interests
- Competition for the market may inhibit the emergence of a successful platform (e.g., CurrentC contract exclusivity requirement)

Privacy issues exemplify competing business models

- Google Wallet
  - Charges the same transaction fees as those on regular payment cards
  - Instead mines payment data to tailor ads
  - Issuers and mobile carriers were wary and slow to adopt
- Apple Pay
  - Charges the same transaction fees as those on regular payment cards
  - Better protects user data and thus attracts customers who highly value privacy
  - Reflects Apple's business model to sell more devices
- CurrentC
  - Shares extensive payment data with merchants, though users retain some control

Cautionary tale of risk in emerging payments

- New stakeholders do not have experience in managing payment fraud
- New payment methods tend to have higher initial rates of fraud
- Apple Pay fraud
  - Insufficient safeguards by some issuers enabled criminals to register stolen cards en masse
  - By one estimate, fraud rate was $6 per $100 charged
  - Apple slow to react and engage with issuers

Bitcoin as an alternative payment platform

- Bitcoin network offers decentralized system that facilitates global payments
- Merchants can accept bitcoin payments on attractive terms: no transaction fees or chargebacks
- To attract consumers, a payment method that avoids currency risk is required
- Payments are inherently more secure through use of cryptography
- Despite novel technology, Bitcoin currently lacks supporting institutions to protect the security of the overall ecosystem, and it is unclear if they can or will be developed

Outline

Concluding remarks

- The biggest challenges facing retail payments security are economic, not technical
- Competing interests and incentives may inhibit adoption of more secure technologies
- Coordination among stakeholders is essential, and game theory can uncover superior outcomes as well as strategies to attain them
- Public authorities, due to long-term vision and societal outlook, can help overcome barriers to collaboration
- Web: `http://lyle.smu.edu/~tylerm/`,
  Email: `tyler-moore@utulsa.edu`