Perspectives on Financial Cryptography

Ronald L. Rivest
MIT Lab for Computer Science
(RSA / Security Dynamics)

FC97 -- 2/27/97

Perspectives on Financial Cryptography (Revisited)

Ronald L. Rivest
MIT Lab for Computer Science
(RSA / Security Dynamics)

FC97 -- 2/27/97

Perspectives on Financial Cryptography (Revisited)

Ronald L. Rivest

MIT Computer Science and AI Lab

(RSA / Security Dynamics)

FC97 -- 2/27/97

Perspectives on Financial Cryptography (Revisited)

Ronald L. Rivest

MIT Computer Science and AI Lab

(RSA)

FC97 -- 2/27/97

Perspectives on Financial Cryptography (Revisited)

Ronald L. Rivest

MIT Computer Science and AI Lab

(RSA)

FC06 – 2/27/06

(1997)

Outline

- I present for your consideration some *debatable propositions* about financial systems and financial cryptography.
- Warning: the propositions expressed may or may not be believed by the author, and may be phrased in a deliberately provocative manner. They may contradict each other.

(2006)

Outline

- I present for your consideration some *debatable propositions* about financial systems and financial cryptography.
- Warning: the propositions expressed may or may not be believed by the author, and may be phrased in a deliberately provocative manner. They may contradict each other.

(OK)

(1997)

Internet money == Interstellar money   (?)

- *P1: There is little difference between Internet payment schemes and interstellar payment schemes.*
- In 2097, you will buy info off the GGG (Grand Galactic Grid) with “starbucks.”

(2006)

Internet money == Interstellar money (?)

- *P1: There is little difference between* *Internet payment schemes* *and* *interstellar payment schemes.*
- **("Starbucks" still a bad pun.)**
- **P1: FALSE (Internet too connected to "real world" (e.g. delivery))**
- ***P1': Need "contact" to learn about "starbucks".***

(1997)

Most schemes don’t work well.

- *P2: Historically, most payment schemes haven’t worked very well.*
- Ref: Weatherford, *History of Money*.
- Commodities (metal, tobacco, wampum, cocoa beans)
  - weighing, purity, quality, deterioration, transportation, storage, theft.
- Coins [Lydia, 630 B.C.]
  - Shaving, debasing, theft, government abuse.

(1997)

Most schemes don’t work well...

- Paper money (China, Italy, U.S. colonies)
  - counterfeiting (scanner/printer), government abuse (inflation), or lack of money
- Checks (England, 1770)
  - Forgery, insolvency, check-washing, ...
- Credit cards (U.S., 1950 Diner’s Club)
  - theft, counterfeiting, non-payment, …
- Electronic money
  - ?? hyperinflation, system collapse, criminal activities protected by anonymity, … ??

(2006)

Most schemes don’t work well.

- *P2: Historically, most payment schemes haven’t worked very well.*
- **P2 still somewhat true.**
- **Hyperinflation in MMORPG’s.**
- **But getting better at “risk management.” (e.g. CYOTA)**
- ***P2’: Payment systems will continue to improve and be more robust and reliable.***

(1997)

Everyone will “make money”

- *P3: Electronic cash systems will enable anyone with a PC to be a “mint” for his own brand of currency.*
- World is becoming more decentralized, more distributed, more “democratic”. (Compare with printing press.)
- Multiple (thousands) of currencies will exist and be traded. Appropriate discount rates will be used for poorly-rated issuers.
- Central banks have a smaller role to play.

(2006)

Everyone will “make money”

- *P3: Electronic cash systems will enable anyone with a PC to be a “mint” for his own brand of currency.*
- **P3 Technically true, but FALSE in practice. Continued dominance of large financial institutions and a few significant currencies.**
- ***P3’: P3 will remain false.***

(1997)

The dollar stays around.

- *P4: National currencies won't go away, to be replaced by cyberspace dollars.*
- Ref: *The Sovereign Individual* (James Davidson and Lord William Rees-Mogg), for contrary view: governments will implode as debts spiral and tax base disappears into cyberspace tax havens.

(2006)

The dollar stays around.

- *P4: National currencies won't go away, to be replaced by cyberspace dollars.*
- **P4: TRUE.**
- ***P4': P4 remains true.***

(1997)

Privacy is already lost

- *P5: Individual privacy is already lost, and must be regained.*
- All information about individual is now electronic form, and is bought and sold.
- There is strong economic incentive for “user profiling” by merchants, card issuers, etc...

(2006)

Privacy is already lost

- *P5: Individual privacy is already lost, and must be regained.*
- **P5 TRUE. Current business and government policies intrude ever more deeply into “personal” realm…**
- ***P5’: People may not care…***

(1997)

User Profiling Not So Bad?

- *P6: User profiling has a definite "up side" for the user:*
  - reduction of unwanted marketing mail; user and advertiser both agree that mail sent should be interesting to user.
  - spending profiles aid fraud detection.

(2006)

User Profiling Not So Bad?

- *P6: User profiling has a definite "up side" for the user.*
- **P6: TRUE. (But only if it works well; my TIVO often guesses my tastes wrong…)**
- ***P6': Benefits of user profiling may become more evident, thus profiling more accepted.***

(1997)

No anonymity for large payments

- *P7: Governments will not allow payment systems to support true (payer or payee) anonymity for large payments.*
- This is for law-enforcement reasons:
  - payer anonymity: bribery, kickbacks, political contributions
  - payee anonymity: extortion, blackmail, kipnapping, etc.
- Anonymity will only work for small payments.

(2006)

No anonymity for large payments

- *P7: Governments will not allow payment systems to support true (payer or payee) anonymity for large payments.*
- **P7: TRUE (especially post 9/11)**
- ***<u>P7’: There is not even serious debate about this anymore.</u>***

(1997)

No anonymity for small payments

- *P8: Achieving payer anonymity for small payments by cryptographic means is too expensive (in terms of complexity and cpu time).*
- Isn’t it just easier to pass very strong privacy-protection laws about the gathering and use of personal spending data?
- But costs decrease over time, too...

(2006)

No anonymity for small payments

- *P8: Achieving payer anonymity for small payments by cryptographic means is too expensive (in terms of complexity and cpu time).*
- **P8 TRUE.**
- ***P8': P8 remains true; while cryptographic approaches to anonymity get more affordable with Moore's Law, anonymity is just not a driver anymore…***

(1997)

Anonymity to be bought and sold

- *P9: Anonymity will be a value-added feature that a user may purchase. Conversely, a user may break his own anonymity in a transaction, for a fee.*
- Most users may feel that anonymity is a good that he should control, and perhaps sell, but not normally a necessity.
- User may reveal his true identity, or else a pseudo-identity (to allow profiling).

(2006)

Anonymity to be bought and sold

- *P9: Anonymity will be a value-added feature that a user may purchase. Conversely, a user may break his own anonymity in a transaction, for a fee.*
- **P9 FALSE.**
- ***P9': P9 remains false. The only thing most users really care about is ease-of-use (convenience).***

(1997)

No multi-app smart cards

- *P10: Multi-application smart cards will never make it big.*
- Coordinating issuers is about as easy as making peace in the Middle East.
- Security issues on a multi-app card are difficult.
- User are comfortable and familiar with having one card per issuer.

(2006)

No multi-app smart cards

- *P10: Multi-application smart cards will never make it big.*
- **P10 TRUE. Some new payment systems appearing (e.g. Dunkin Donuts prepaid card)**
- **There are some signs that this may change: "octopus card" in Hong Kong…**
- ***P10': Cell phone will become your multi-app "smart card"***

(1997)

Anonymity by smart-card choice

- *P11: Anonymity for small-value payments will arise (only) from anonymity of card-holder/card relationship.*
- Smart cards can be obtained anonymously, as frequently as desired.
- Smart card ID is a pseudonym for user. (Nyms are already understood by AOL users…)

(2006)

Anonymity by smart-card choice

- *P11: Anonymity for small-value payments will arise (only) from anonymity of card-holder/card relationship.*
- **P11 TRUE. Small pre-paid application cards (e.g. for transit) provide some anonymity.**
- ***P11': P11 remains true.***

(1997)

Cost of breaking SC’s to rise

- *P12: Smart cards will be “broken into” on a regular basis, but the cost of doing so will rise dramatically over the next decade.*
- Smaller feature sizes make requisite lab equipment more expensive.
- Vast number of installed smart cards will stimulate further investment into security measures and lower production costs.
- Compare: bank safes.

(2006)

Cost of breaking SC’s to rise

- *P12: Smart cards will be “broken into” on a regular basis, but the cost of doing so will rise dramatically over the next decade.*
- **P12: TRUE. (Depending on def’n of “regular”) We are presumably getting better at designing secure chips.**
- ***P12’: RFID chip security will be the most interesting battleground. (These are not so “smart”, but they will be pervasive.)***

(1997)

No large-value digital coins

- *P13: Digital coins will not be used for large-value transactions.*
- In a coin-based system (as opposed to an account-based system), possession of bits means possession of value. Replication!
- Identification of double-spenders is unlikely to be a sufficient deterrent to prevent major fraud. (Compare with credit-card theft .)

(2006)

No large-value digital coins

- *P13: Digital coins will not be used for large-value transactions.*
- **P13 TRUE (also true for small-value; digital coins aren’t being used at all).**
- ***P13’: Digital coins will never make it – all electronic payment systems will essentially “account-based”.***

(1997)

No transferable coins!

- *P14: Payment schemes with off-line coin transfers between users won't make it.*
- Need will decrease dramatically as every device and individual can be "on-line" whenever it wants to.
- No good business model: what does issuer gain by allowing transferability? (Extra "float" doesn't compensate for extra risk. Compare with early US bank notes...)

(2006)

No transferable coins!

- *P14: Payment schemes with off-line coin transfers between users won't make it.*
- **P14 TRUE.**
- ***P14': (Same as P13': digital coin systems won't make it in general.)***

(1997)

Micropayments will thrive

- *P15: Micropayment schemes will be the system of choice for purchasing most information over the Web.*
- Most information is low-value (<10 cents).
- Significant “price umbrella” underneath credit-card transactions (29 cents + 2%).
- Latency of response is important. (Not enough time for “serious crypto”.)

(2006)

Micropayments will thrive

- *P15: Micropayment schemes will be the system of choice for purchasing most information over the Web.*
- **P15 FALSE. Ad-based systems dominate micropayment schemes for this purpose.**
- ***P15’: While “small payment” schemes may thrive, true “micro” payment schemes may never make it. (Note Peppercoin now focuses on “small payments” not “micropayments”…)***

(1997)

General PKI's not necessary

- *P16: General-purpose public-key infrastructures (PKI's) are not necessary for financial cryptography---they can (and will) be special-cased.*
- Name/key binding may be less important than attribute binding (e.g. account is in good standing; merchant has few problems).

(2006)

General PKI’s not necessary

- *P16: General-purpose public-key infrastructures (PKI’s) are not necessary for financial cryptography---they can (and will) be special-cased.*
- **P16 TRUE.**

(1997)

Money and voting are close.

- *P17: Voting systems and payment systems will be seen as being very close.*
- Voting for candidate is like giving $1 coin to candidate so she can bid for and “buy” election. (Special “registrar currency”.)
- Anonymity of voting is *necessary*. (This is a great example against key escrow or key recovery.)

(2006)

Money and voting are close.

- *P17: Voting systems and payment systems will be seen as being very close.*
- **P17 FALSE. The closer one looks at voting, the more the similarities seem superficial. (E.g. "selling one's vote" has no real counterpart; "trusted third parties" are perhaps less trusted; no analogue for "universal verification", etc.)**

(1997)

You can get anything you want...

- *P18: "Alice's crypto restaurant" can serve up any feasible combination of system requirements at a workable cost (not necessarily cheap).*
- Be careful what you ask for…
- Some problems are not technical, but socio-political (whom do you trust?---key recovery, etc.)

(2006)

You can get anything you want...

- *P18: "Alice's crypto restaurant" can serve up any feasible combination of system requirements at a workable cost (not necessarily cheap).*
- **P18 TRUE. (Even more so with magic of elliptic curves and bilinear maps in many cases.)**

(2006)

How did I do?

- 13/18 TRUE… I get a “B”…??
- More important than accuracy: were the questions good ones?
- Scientists are typically over-optimistic in short term, but wildly under-optimistic in long term…

(1997)

Conclusions

- “Financial cryptography” is an essential component of electronic payment schemes.
- Such schemes will augment and largely replace many existing payment schemes, and will offer new features (selective anonymity, interstellar payments…)

(2006)

Conclusions

- 1997 was an “optimistic” year, with too much emphasis on anonymity!
- The gap between the “science” of financial cryptography and the “practice” of financial transactions is large – perhaps our job is to make it even larger (!), by continuing to explore “what is possible”. Practice may (or may not) follow…