Legislating digital signatures: Lessons from a past cryptographic utopia

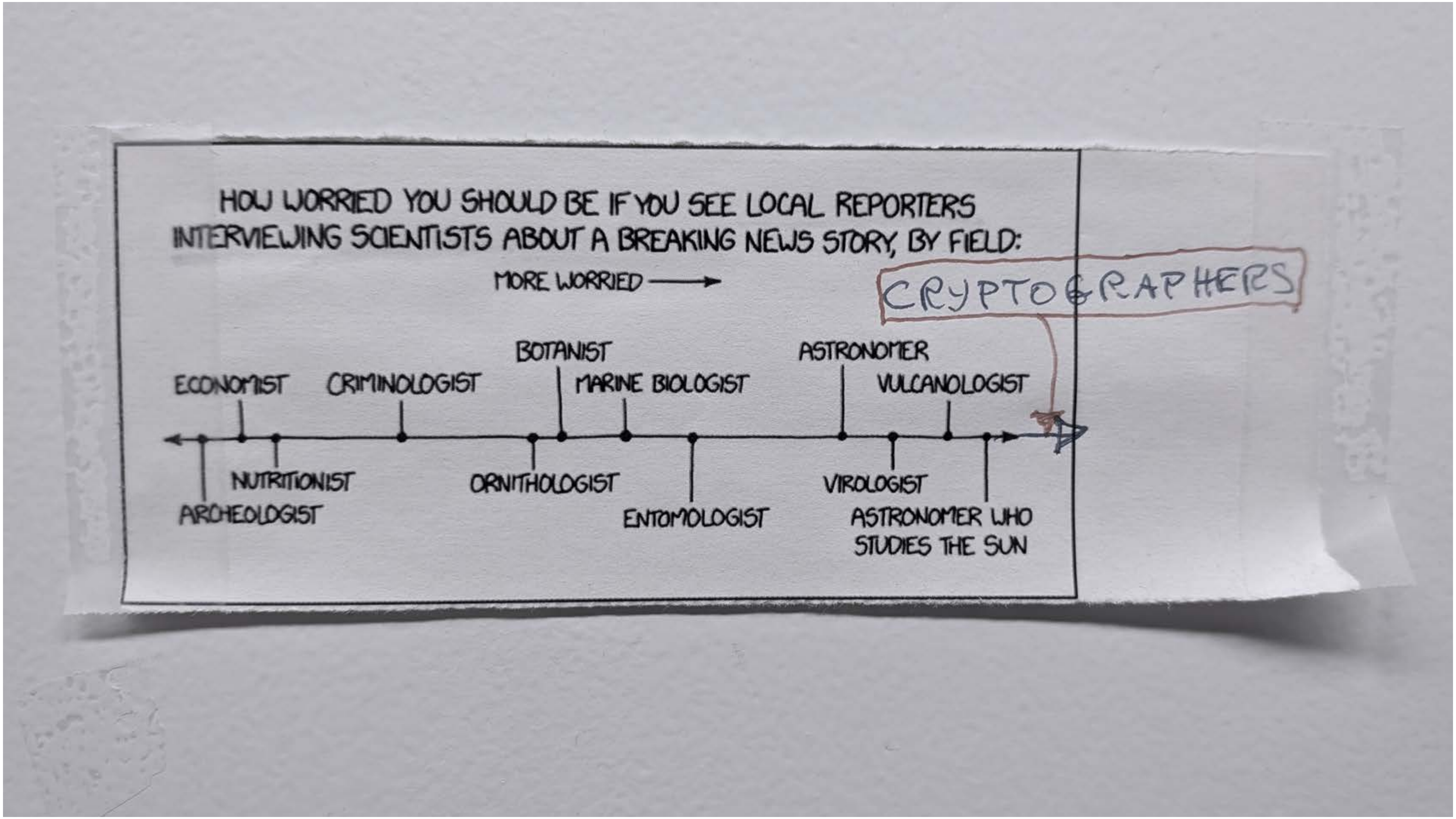
Jean-François Blanchette

École nationale supérieure des sciences de l'information et des bibliothèques (Enssib)

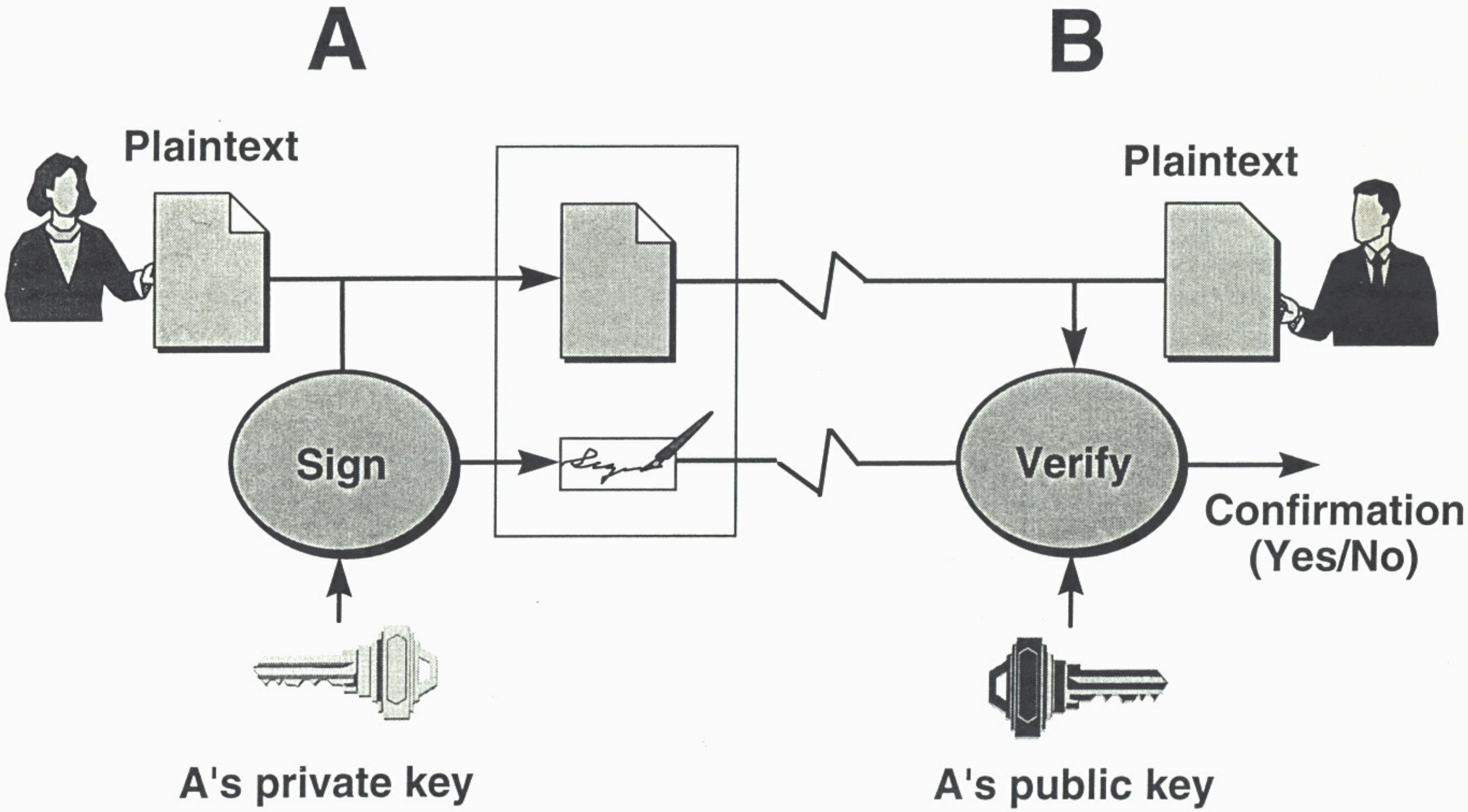
Department of Information Studies, UCLA

Cryptology and Social Life Workshop, NTNU

December 11, 2025


HOW WORRIED YOU SHOULD BE IF YOU SEE LOCAL REPORTERS INTERVIEWING SCIENTISTS ABOUT A BREAKING NEWS STORY, BY FIELD:
MORE WORRIED →
ECONOMIST
ARCHEOLOGIST
NUTRITIONIST
CRIMINOLOGIST
ORNITHOLOGIST
BOTANIST
MARINE BIOLOGIST
ENTOMOLOGIST
ASTRONOMER
VIROLOGIST
VULCANOLOGIST
ASTRONOMER WHO STUDIES THE SUN
CRYPTOGRAPHERS

Digital Signature



A

B

Plaintext

Plaintext

Sign

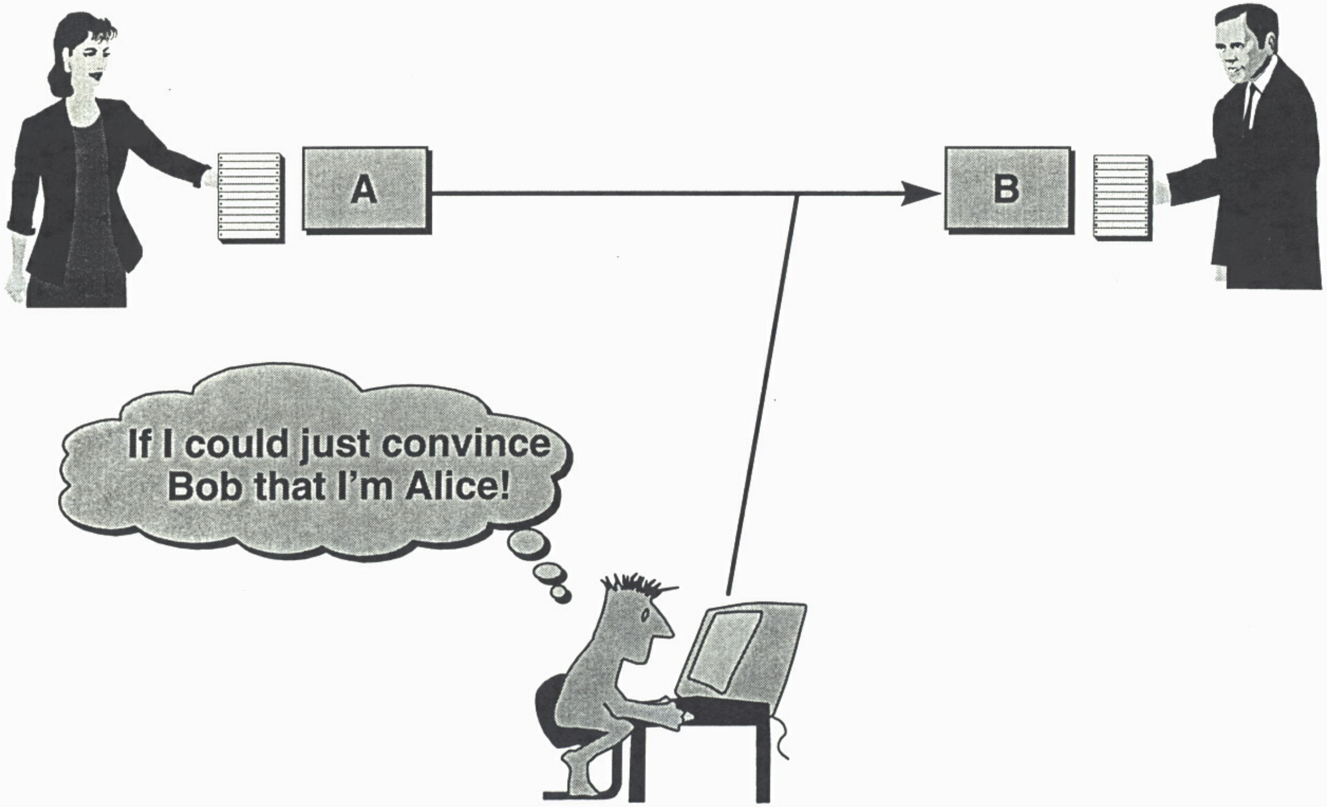
Verify

Confirmation (Yes/No)

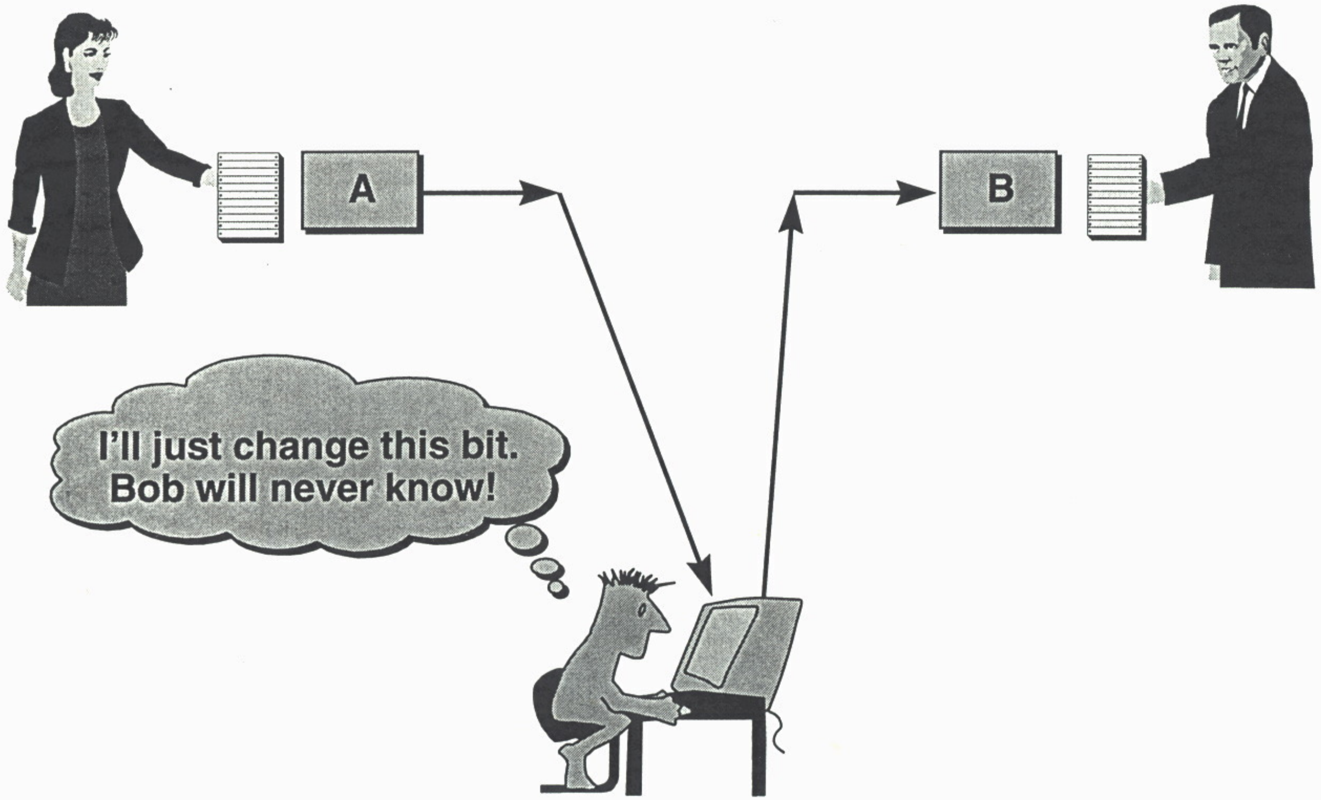
A's private key

A's public key

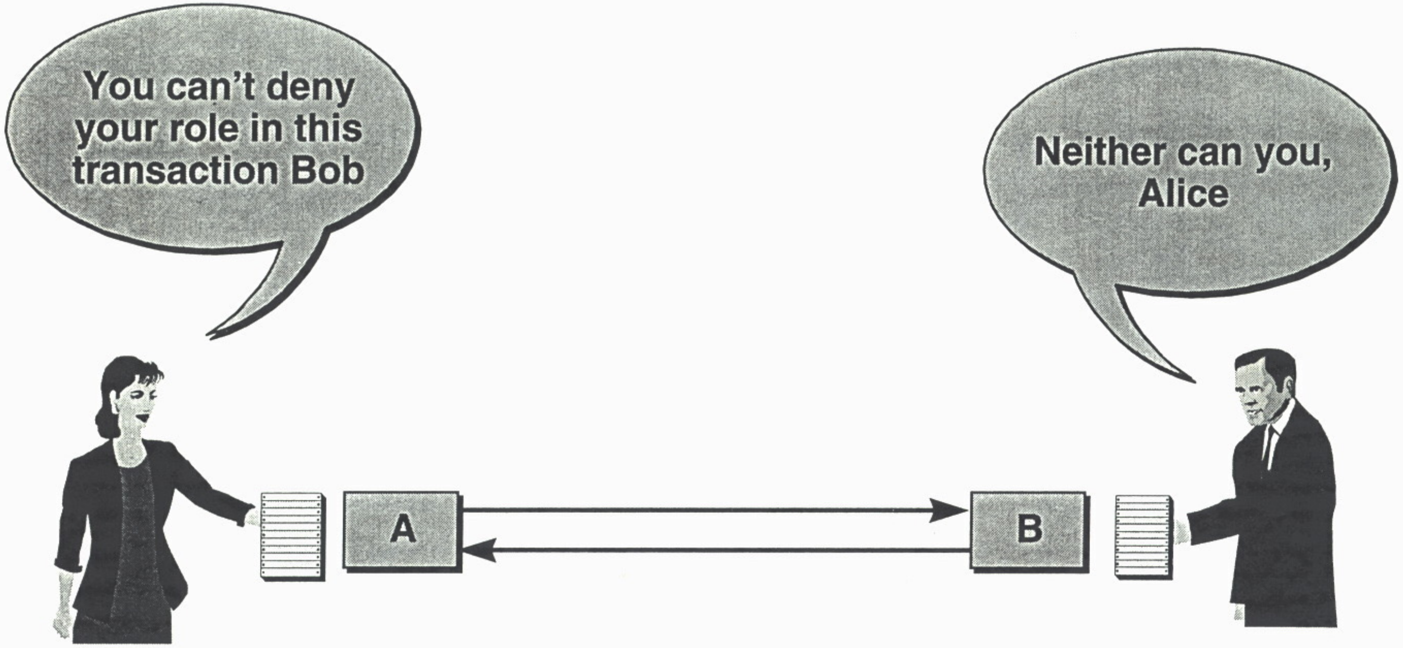
Authentication



Integrity



Non-Repudiation



DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 13 December 1999

on a Community framework for electronic signatures

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Articles 47(2), 55 and 95 thereof,

Having regard to the proposal from the Commission [1],

Having regard to the opinion of the Economic and Social Committee [2],

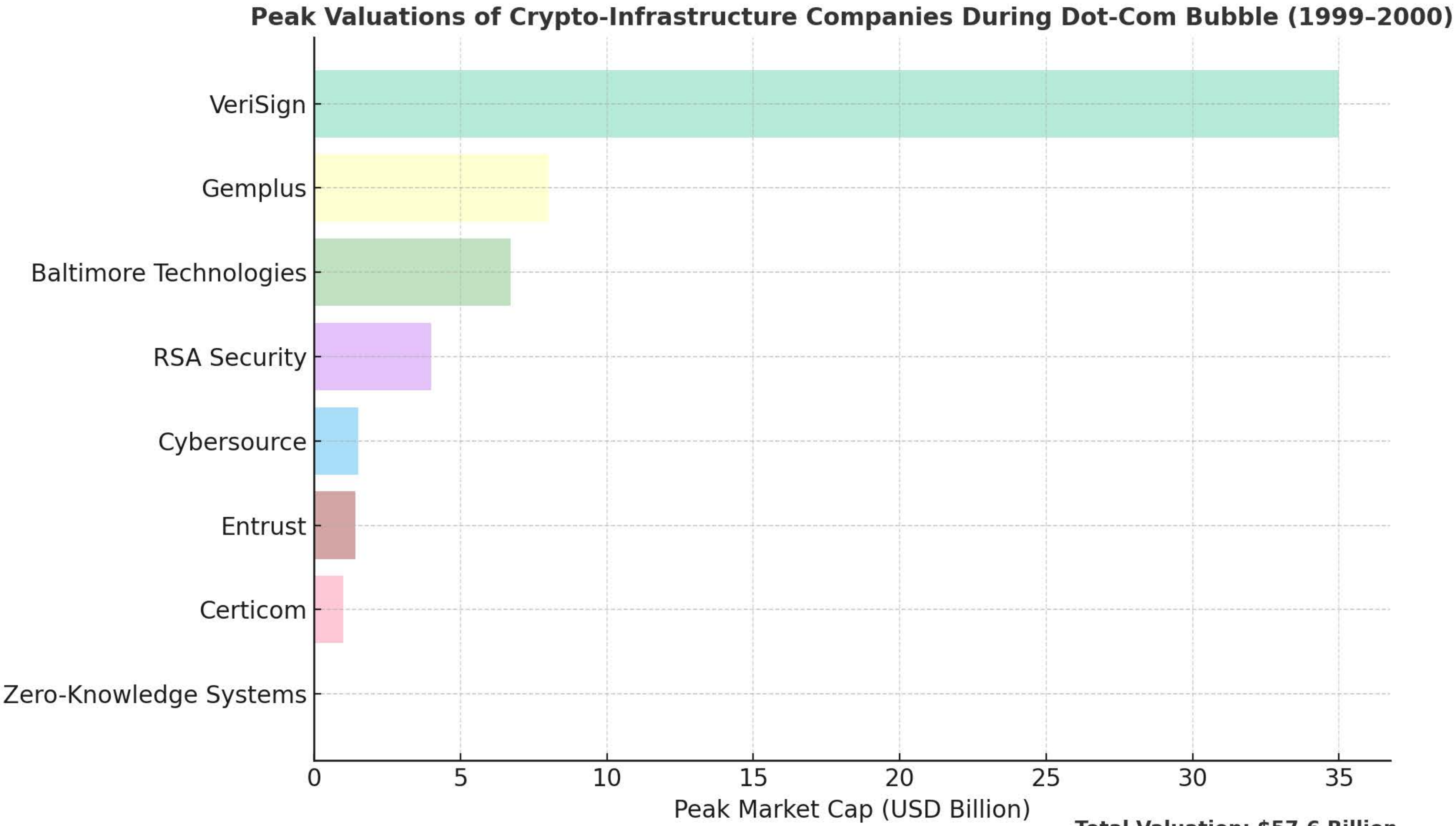
Having regard to the opinion of the Committee of the Regions [3],

Acting in accordance with the procedure laid down in Article 251 of the Treaty [4],

Whereas:

(5) The interoperability of electronic-signature products should be promoted; in accordance with Article 14 of the Treaty, the internal market comprises an area without internal frontiers in which the free movement of goods is ensured; essential requirements specific to electronic-signature products must be met in order to ensure free movement within the internal market and to build trust in electronic signatures, without prejudice to Council Regulation (EC) No 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods [5] and Council Decision 94/942/CFSP of 19 December 1994 on the joint action adopted by the Council concerning the control of exports of dual-use goods [6];

(6) This Directive does not harmonise the provision of services with respect to the confidentiality of information where they are covered by national provisions concerned with public policy or public security;



Total Valuation: $57.6 Billion

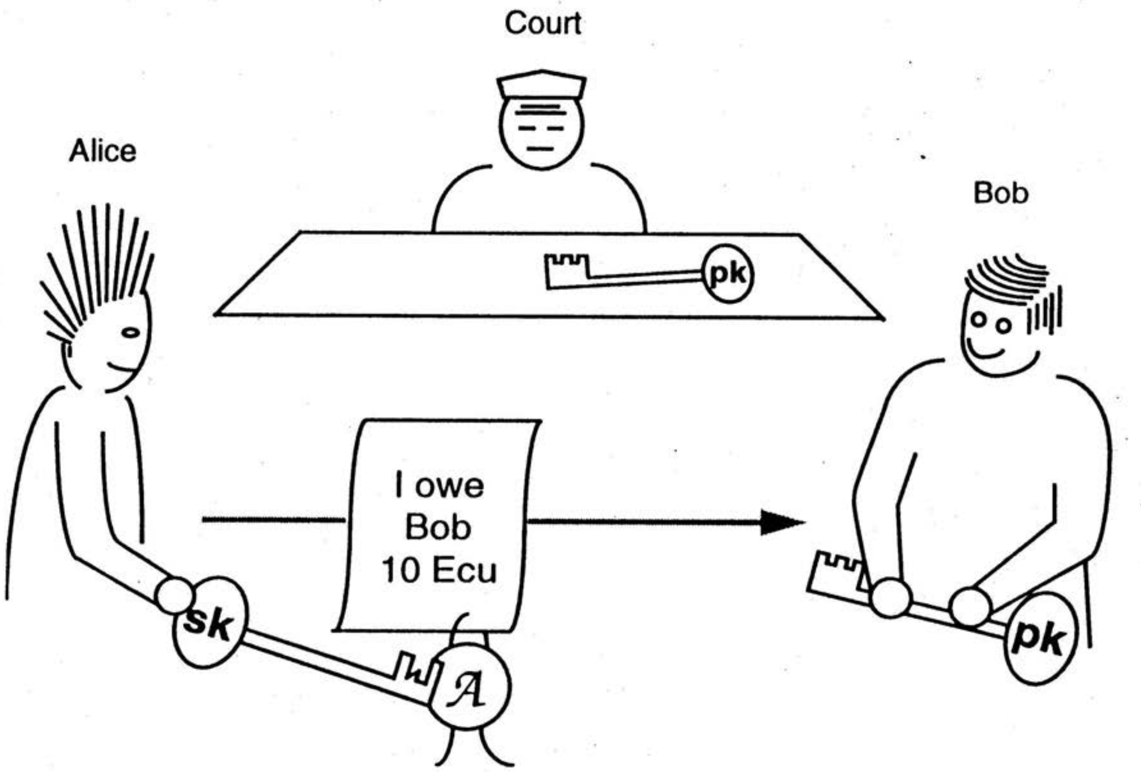
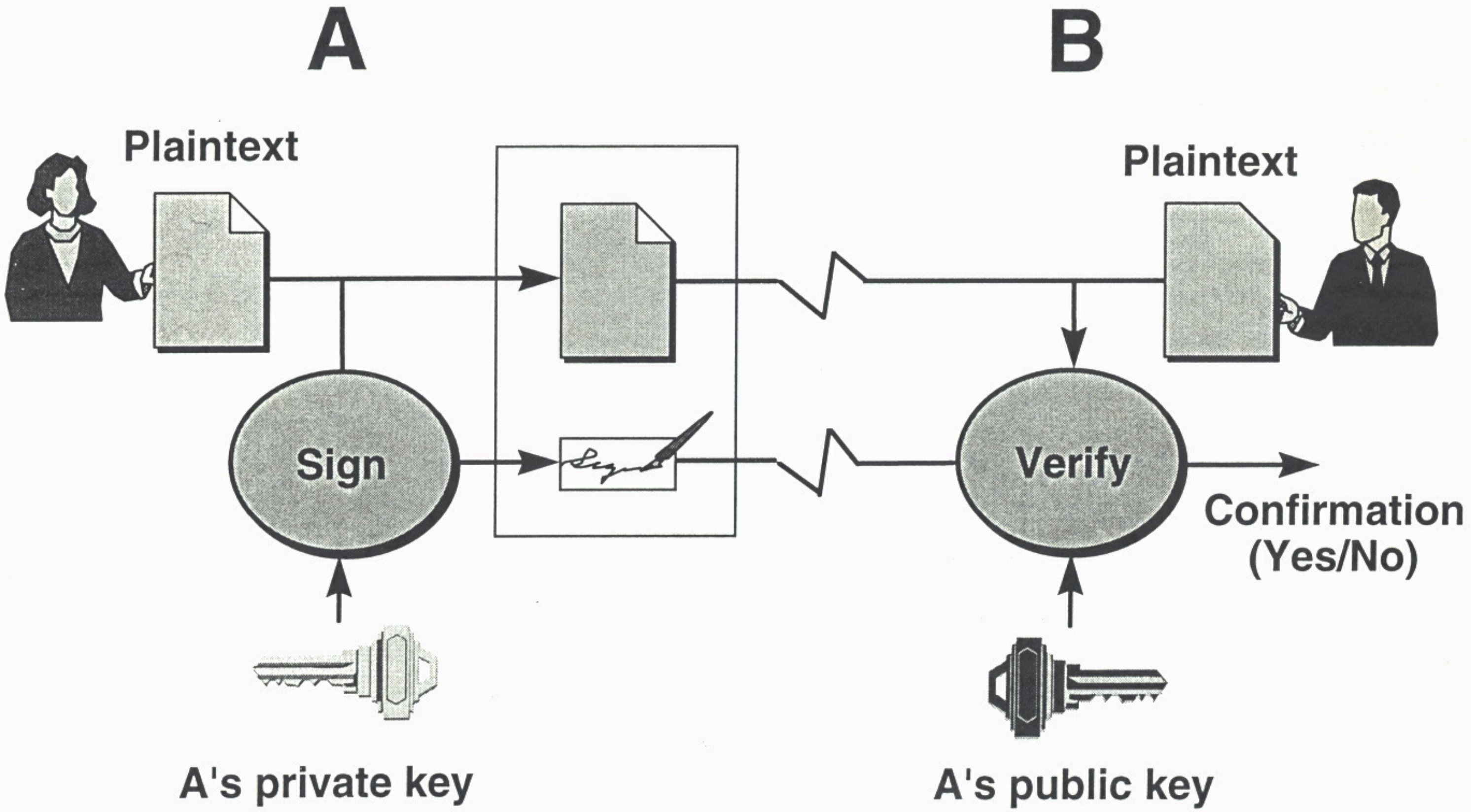
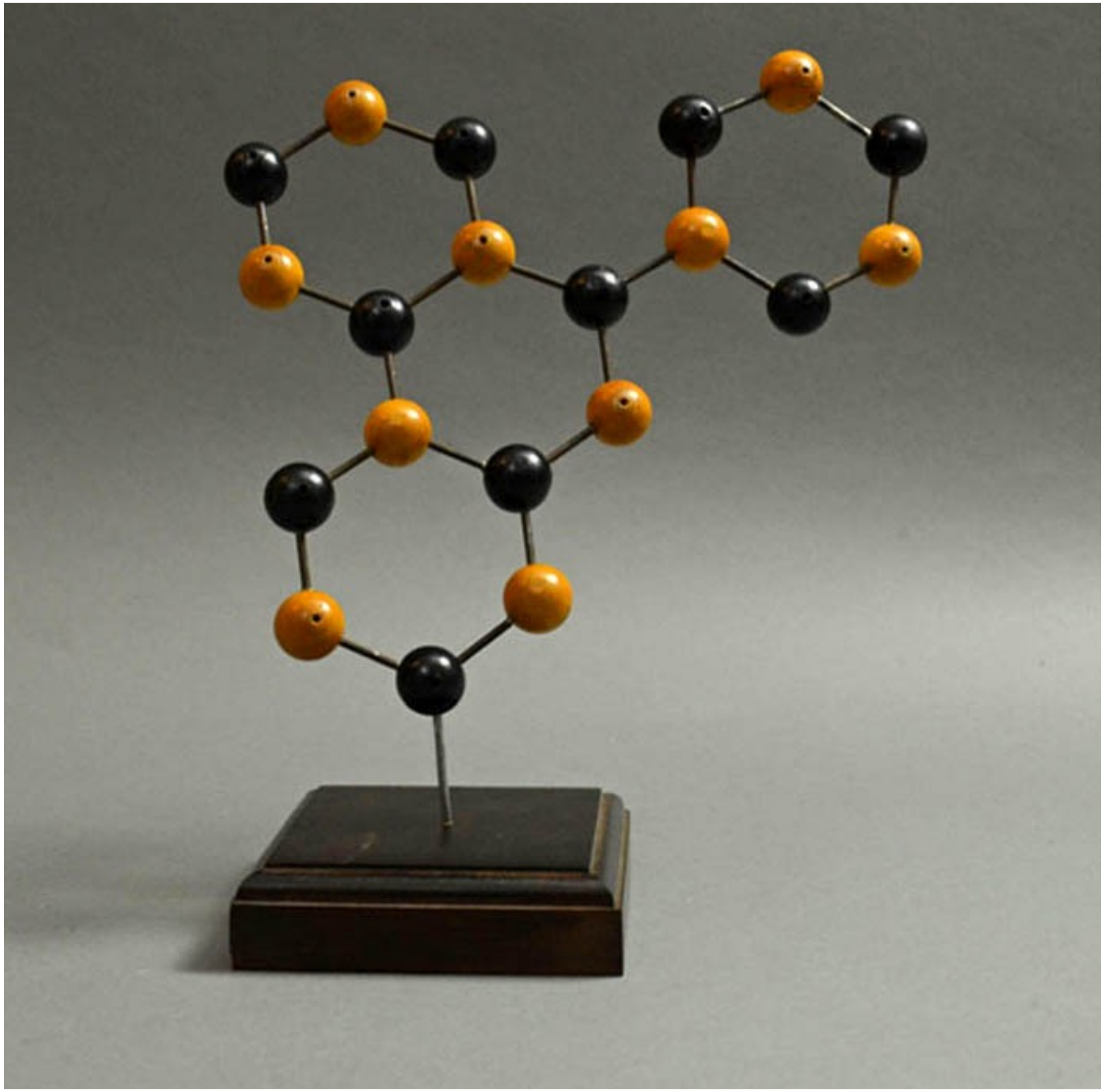
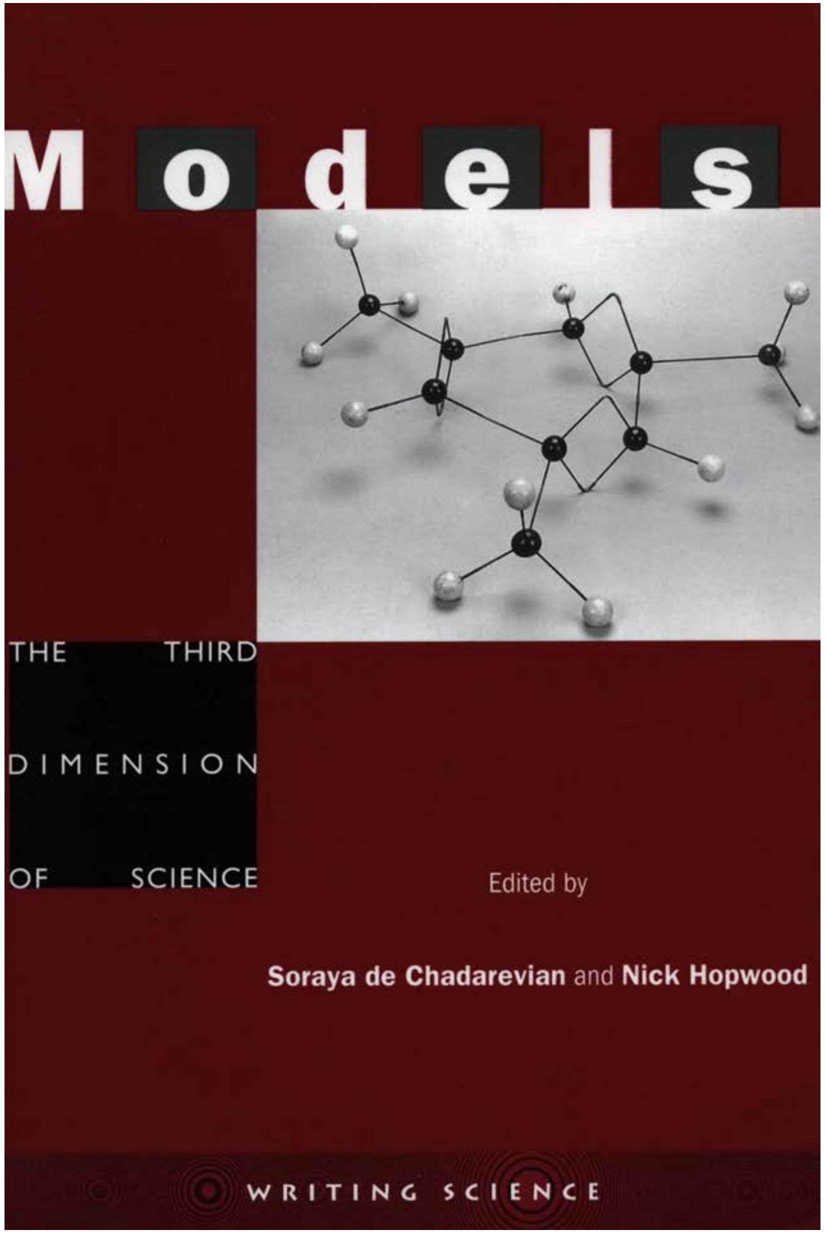


Figure 2.1. Components of ordinary digital signature schemes.
In the example, Alice has chosen a key pair (*sk*, *pk*) and published *pk*. In particular, Bob and the court know *pk*. Now, only Alice can sign her message with *sk*. Bob and the court accept a message as signed by Alice if and only if it passes the test with *pk*.

Digital Signature







Models

THE THIRD DIMENSION OF SCIENCE

Edited by

Soraya de Chadarevian and Nick Hopwood

WRITING SCIENCE

3 confrontations

- Crypto vs law:
  - How did the law understand and modelled cryptographic signatures?
  - What kind of evidential power did it grant them?
- Crypto vs users:
  - How did users (legal professions) understand cryptographic signatures?
  - How did they integrate them within their professional practices?
- Crypto vs crypto:
  - How did the cryptographic signature model emerge?
  - Where does the design mandate for the field come from?
  - What do internal debates reveal about the field’s boundaries and program?

Part 1:
Crypto vs law

UNCITRAL Model Law on E-Commerce

- Enacted in 1996, with the aim of facilitating the use of modern means of communications and storage of information in international trade
- “Functional definition” of signatures: the signing method must enable one to:
  - identify the signer and
  - indicate that the signer manifests her consent
- Non-discrimination principle:
  - “Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message”

ABA “Digital Signature Guidelines”

- Proposed in 1996, to help US State legislatures in the elaboration of digital signature bills
- Exclusively defined electronic signatures as those based on cryptographic signatures:
  - “Digital signatures, as those used in these guidelines, does not include the results of encryption and decryption by means other than an asymmetric cryptosystem, nor does it include a digitized version of a handwritten signature, a typewritten signature, such as ‘John Doe’, the use of passwords of other practices for controlling access, or any other computer-based representation of identity or authentication.”
- Cryptographic signatures granted a presumption of trustworthiness, leading to a reversal of burden of proof

DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 13 December 1999

on a Community framework for electronic signatures

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Articles 47(2), 55 and 95 thereof,

Having regard to the proposal from the Commission [1],

Having regard to the opinion of the Economic and Social Committee [2],

Having regard to the opinion of the Committee of the Regions [3],

Acting in accordance with the procedure laid down in Article 251 of the Treaty [4],

Whereas:

(5) The interoperability of electronic-signature products should be promoted; in accordance with Article 14 of the Treaty, the internal market comprises an area without internal frontiers in which the free movement of goods is ensured; essential requirements specific to electronic-signature products must be met in order to ensure free movement within the internal market and to build trust in electronic signatures, without prejudice to Council Regulation (EC) No 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods [5] and Council Decision 94/942/CFSP of 19 December 1994 on the joint action adopted by the Council concerning the control of exports of dual-use goods [6];

(6) This Directive does not harmonise the provision of services with respect to the confidentiality of information where they are covered by national provisions concerned with public policy or public security;

European Directive on E-Signatures

- Enacted in 1999 by the European Commission, in order to prevent obstacles to the Common Market
- Hoped to do for authentication services what GSM did for the cellular telephony market in Europe
- Binding on all member States, but obligation of results, not of means
- Aspired to “technological neutrality” but also attempted to provide favorable conditions to the most mature technology, i.e., cryptographic signatures

European Directive on E-Signatures

- “Simple” electronic signature:
  - “data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication”
- “Advanced” electronic signatures have additional features:
  - uniquely linked to the signatory
  - created using means that the signatory can maintain under his sole control;
  - linked to the data to which it relates in such a way that any subsequent change of the signed data is detectable.
- To each type is associated a different evidential regime:
  - “Simple” are admissible (non-discrimination principle), but with no specified proof value
  - Advanced are admissible + have identical weight as handwritten signatures

LOIS

LOI n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (1)

NOR : *JUSX9900020L*

L'Assemblée nationale et le Sénat ont adopté,

Le Président de la République promulgue la loi dont la teneur suit :

Article 1er

I. – L'article 1316 du code civil devient l'article 1315-1.

II. – Les paragraphes 1er, 2, 3, 4 et 5 de la section 1 du chapitre VI du titre III du livre III du code civil deviennent respectivement les paragraphes 2, 3, 4, 5 et 6.

III. – Il est inséré, avant le paragraphe 2 de la section 1 du chapitre VI du titre III du livre III du code civil, un paragraphe 1er intitulé : « Dispositions générales », comprenant les articles 1316 à 1316-2 ainsi rédigés :

« *Art. 1316.* – La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités

« Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat. »

Article 5

A l'article 1326 du code civil, les mots : « de sa main » sont remplacés par les mots : « par lui-même ».

Article 6

La présente loi est applicable en Nouvelle-Calédonie, en Polynésie française, à Wallis-et-Futuna et dans la collectivité territoriale de Mayotte.

La présente loi sera exécutée comme loi de l'Etat.

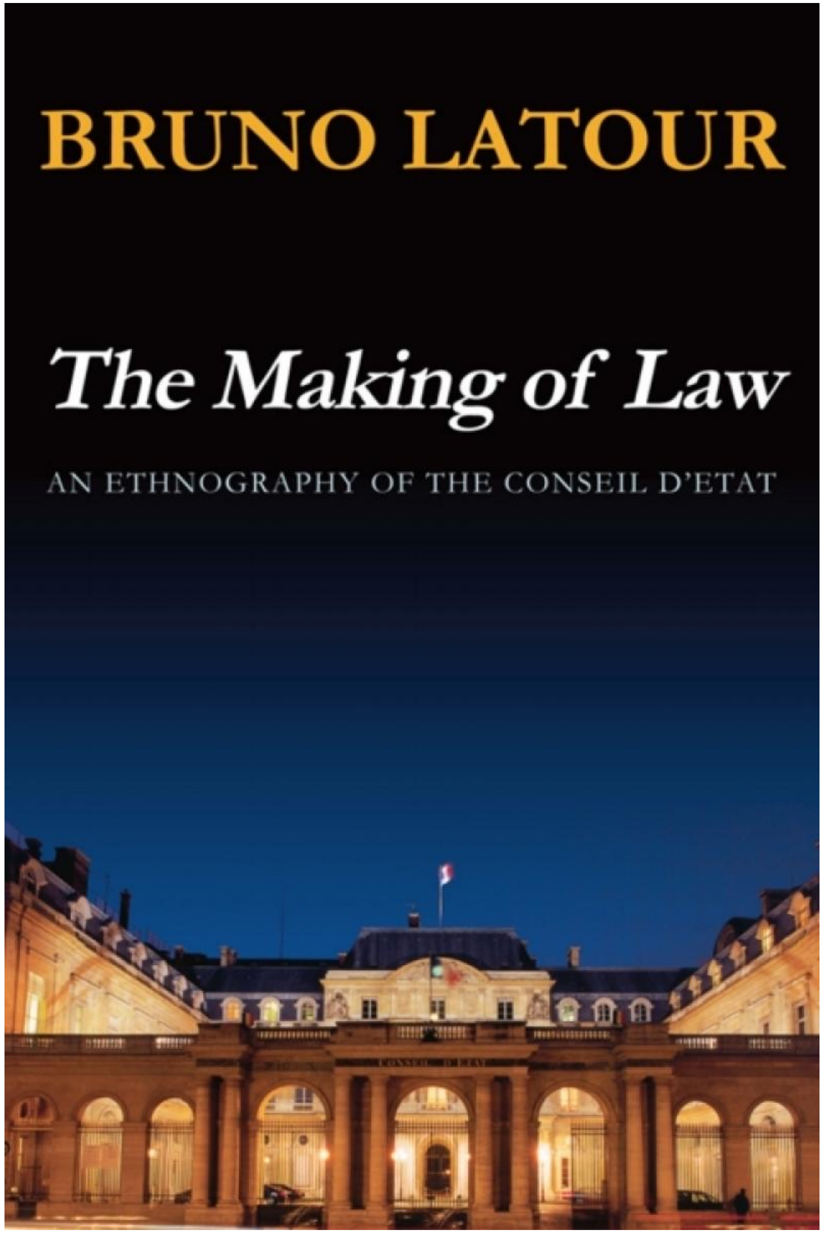
Fait à Paris, le 13 mars 2000.

JACQUES CHIRAC

Par le Président de la République :

French signatures (March 2000 bill)

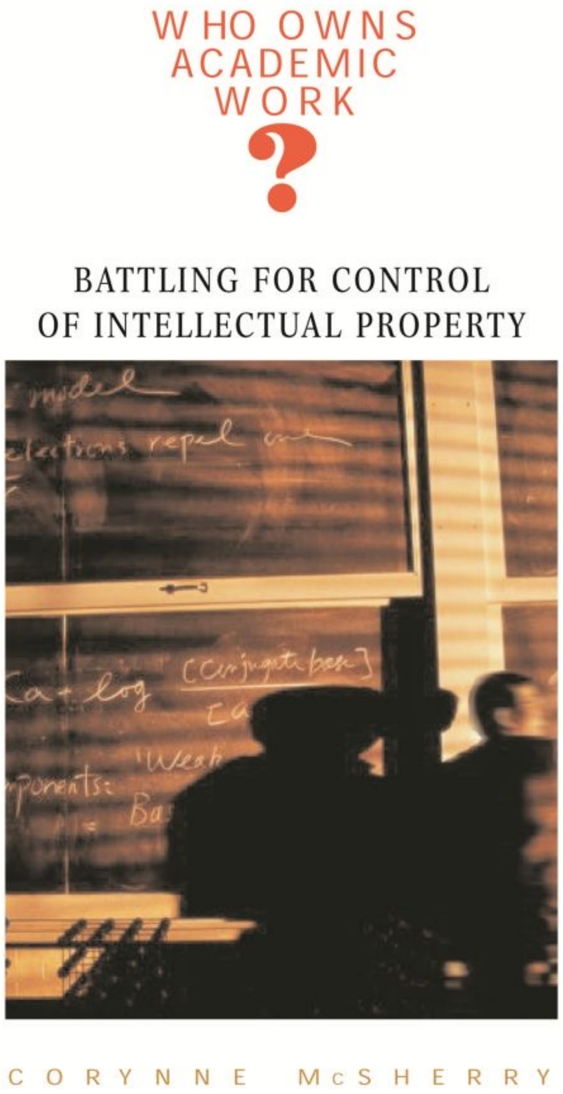
- Define writing as independent of any media — “Literal proof, or proof in writing, results from a sequence of letters, characters, numbers, or any other signs or symbols endowed with an intelligible meaning, whatever their medium or means of transmission.”
- “Writing on electronic media has the same probative value as writing on paper.”
- Only a rebuttable presumption of reliability:
  - “When it is electronic, it consists in the use of a trustworthy identification mechanism guaranteeing the link with the act to which the signature is attached.
  - *The trustworthiness of this mechanism is presumed, until proof of the contrary*, when the signature is created, the identity of the signatory ensured, and the integrity of the act guaranteed, under conditions established by a decree from the *Conseil d'état*.”
- Judge can be convinced otherwise when presented with contrary evidence



BRUNO LATOUR

The Making of Law

AN ETHNOGRAPHY OF THE CONSEIL D'ETAT



WHO OWNS ACADEMIC WORK?

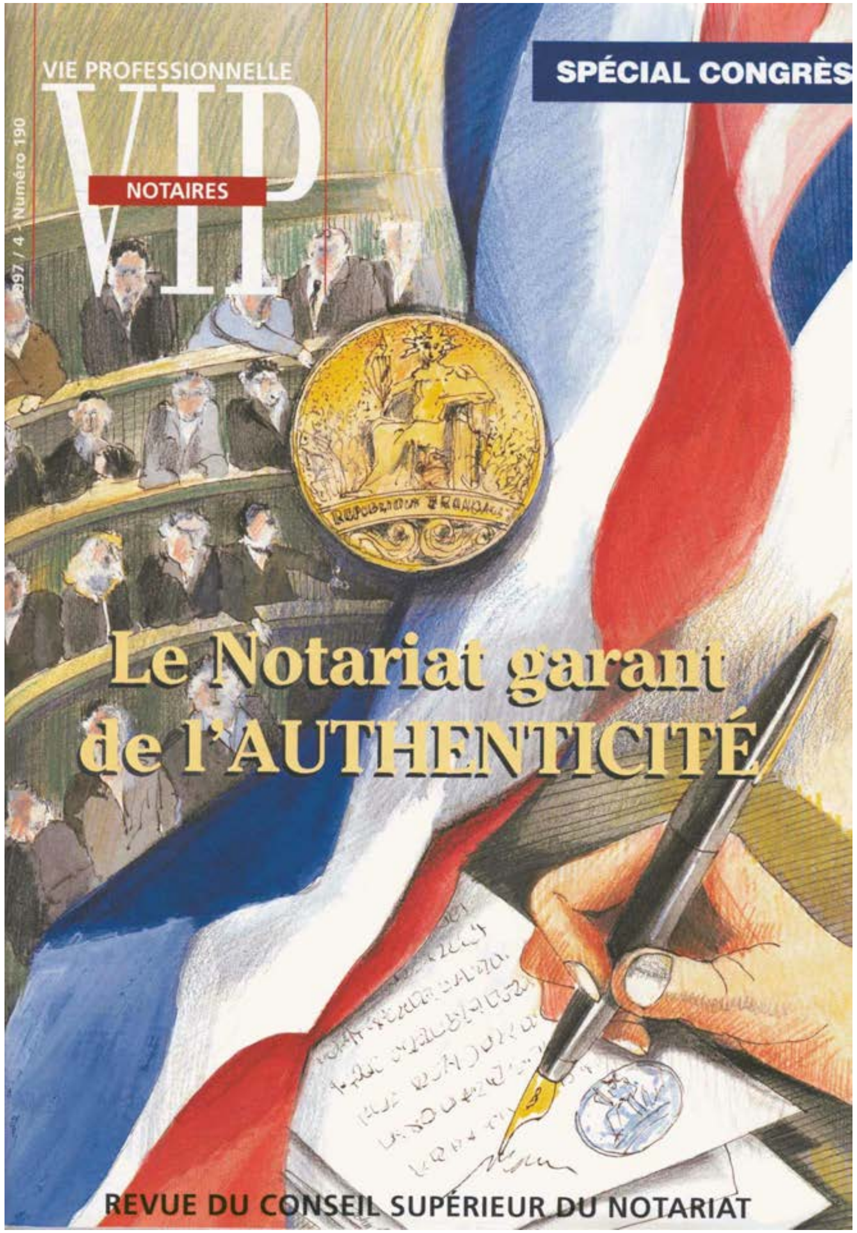
BATTLING FOR CONTROL OF INTELLECTUAL PROPERTY

CORYNNE McSHERRY

Part 2:
Crypto vs users

‘Authentic’ acts

- France has a two-level hierarchy of written proof: regular and *authentic* - notarized contracts; records of civil status; court decisions;
  - Drafted by and under the care of a trusted witness, the public officer;
  - Must meet extensive form requirements;
  - Testify of their origin, date, and content *in and of themselves*;
  - No limits on duration of archiving.
- *Civil Code, Art. 1317* — “The authentic act is that one which has been received with the required solemnities by an authorized public officer. *It can be established on electronic media if it is drafted and preserved under conditions established by decree from the Conseil d'état.*”



VIE PROFESSIONNELLE

VIP

NOTAIRES

1997 / 4 - Numéro 190

SPÉCIAL CONGRÈS

Le Notariat garant de l'AUTHENTICITÉ

REVUE DU CONSEIL SUPÉRIEUR DU NOTARIAT

Notaires

VIE PROFESSIONNELLE

«TOUTE LA FAMILLE» AU CONGRÈS DE MARSEILLE

CHEZ LE NOTAIRE QUI PAIE QUOI ?

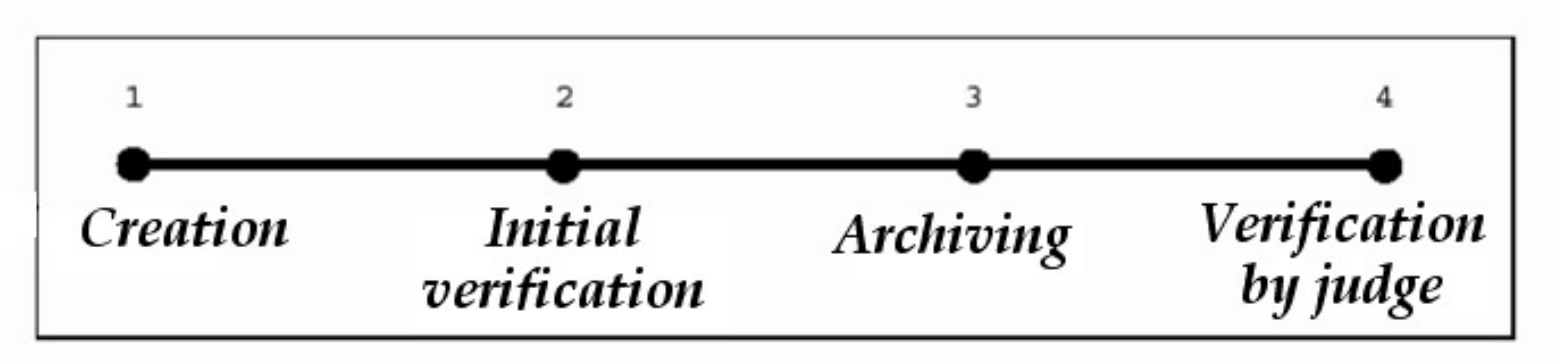
LA CONVENTION COLLECTIVE ET LES 35 HEURES

La carte du réseau électronique notarial

REVUE DU
CONSEIL SUPÉRIEUR
DU NOTARIAT
1999 / 4 - Numéro 207

Figure 6.4
Rachida Dati, Minister of Justice and Keeper of the Seals, in 2008 signs the first electronic authentic act using a graphical pad. Photograph by Luc Pérénom, courtesy of the Conseil supérieur du notariat.

Electronic signature lifecycle



- To serve as evidence, digital signatures must be trustworthy during **both** initial verification and verification in the course of litigation
- Archiving electronic documents is not a neutral process

The fundamental dilemma

- Digital signature verification fails if a single bit of the document is modified after being signed, *whether the modification is malicious or effected for purposes of preservation.*
- Preserving digital signatures makes impossible any migration of a document's logical encoding, forever freezing it in its original state
- Furthermore, digital signatures are electronic data which must also be preserved so as to be meaningful in the future

Trusted Archival Services

- Proposed by the EESSI standardization consortium
- A new type of commercial service that would be offered by competent bodies and professions, to guarantee the long-term integrity of cryptographi-cally signed documents
- Technical requirements:
  - “to guarantee that the content of the documents can still be viewed and that the signature on these documents can still be validated years later …
  - … TAS should provide **backward compatible service**, i.e., maintain a set of applications (viewers as well as signature validation applications) together with the corresponding platforms (hardware, operating systems, etc), or at least an emulator of such applications”

Resignature

- EESSI “Electronic Signature Formats” distinguishes between “initial validation” and “late validation” (steps 2 and 4 of the signature lifecycle)
- “Archive” signature format encapsulates all of the information that can be eventually used in the late validation process, such as public key certificates, revocation information, timestamps, etc.
- Primary security threat to the validity of digital signatures modeled as decay in cryptographic strength:
  - “Before the algorithms, keys and other cryptographic data used at the time the electronic signature was built become weak and the cryptographic functions become vulnerable, the signed data should be timestamped … using stronger algorithms (or longer key lengths) than in the original timestamp.”

NARA guidelines

- “the agency’s preserves the signature’s validity and meets the adequacy of documentation requirements by retaining the contextual information that documented the validity of the electronic signature at the time the record was signed.”
- Or … preserves the ability to validate signatures, “an approach potentially more burdensome, particularly for digitally-signed records with long retention needs, due to issues of hardware and software obsolescence.”
- In all cases … “agencies must ensure that the printed name of the electronic signer, as well as the date when the signature was executed, be included as part of any human readable form (i.e., electronic display or printout) of the electronic form.“

National Archives of Canada

- Guidelines relatives to the preservation of encrypted and digitally signed documents published in 2001
- “The National Archives will not attempt to maintain the capacity to re-verify a digital signature after transfer to its control, nor to preserve the traces of a digital signature generated under the current federal PKI system.”
- “For National Archives' purposes, the integrity and authenticity of records will continue to be inferred from their placement within an organization's record-keeping system during the normal course of business, and from proof of that organization's reliance on records kept within their record-keeping system.”

InterPARES

- “Digital signatures and PKI are examples of technologies that have been developed as a means of authentication for electronic records transmitted **across space**. … These technologies were never intended to be, and are not currently viable, as a means for ensuring the authenticity of electronic records **over time**.”
- It is not possible to preserve an electronic record as a stored physical object: it is only possible to preserve the ability to reproduce (make manifest) the record.
- The entire process of preservation must be thoroughly documented as a primary means for protecting and assessing authenticity over the long term.

Two views of electronic evidence

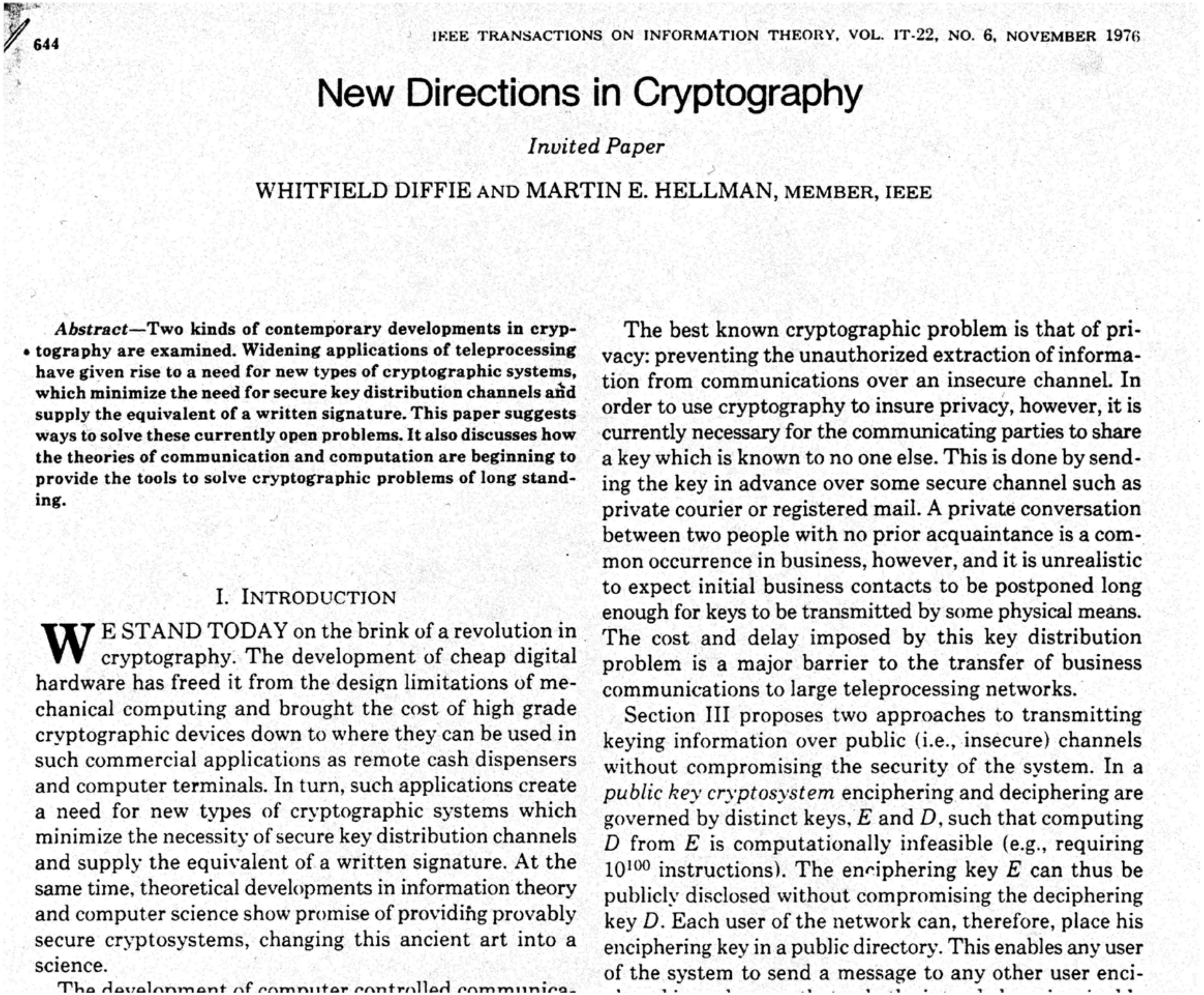
Physical measures:

- Authenticity = bitwise integrity
- Integrity ensured by trusted cryptographic technology
- Signature verification is primary evidence

Contextual measures:

- Authenticity = probabilistic measure of all available evidence
- Integrity ensured by trusted custodian, through whatever means necessary, including migration of underlying bitstring
- Signature verification is just one piece of metadata

Part 3:
Crypto vs Crypto



644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

***Abstract*—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.**

I. INTRODUCTION

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.

The development of computer controlled communica-

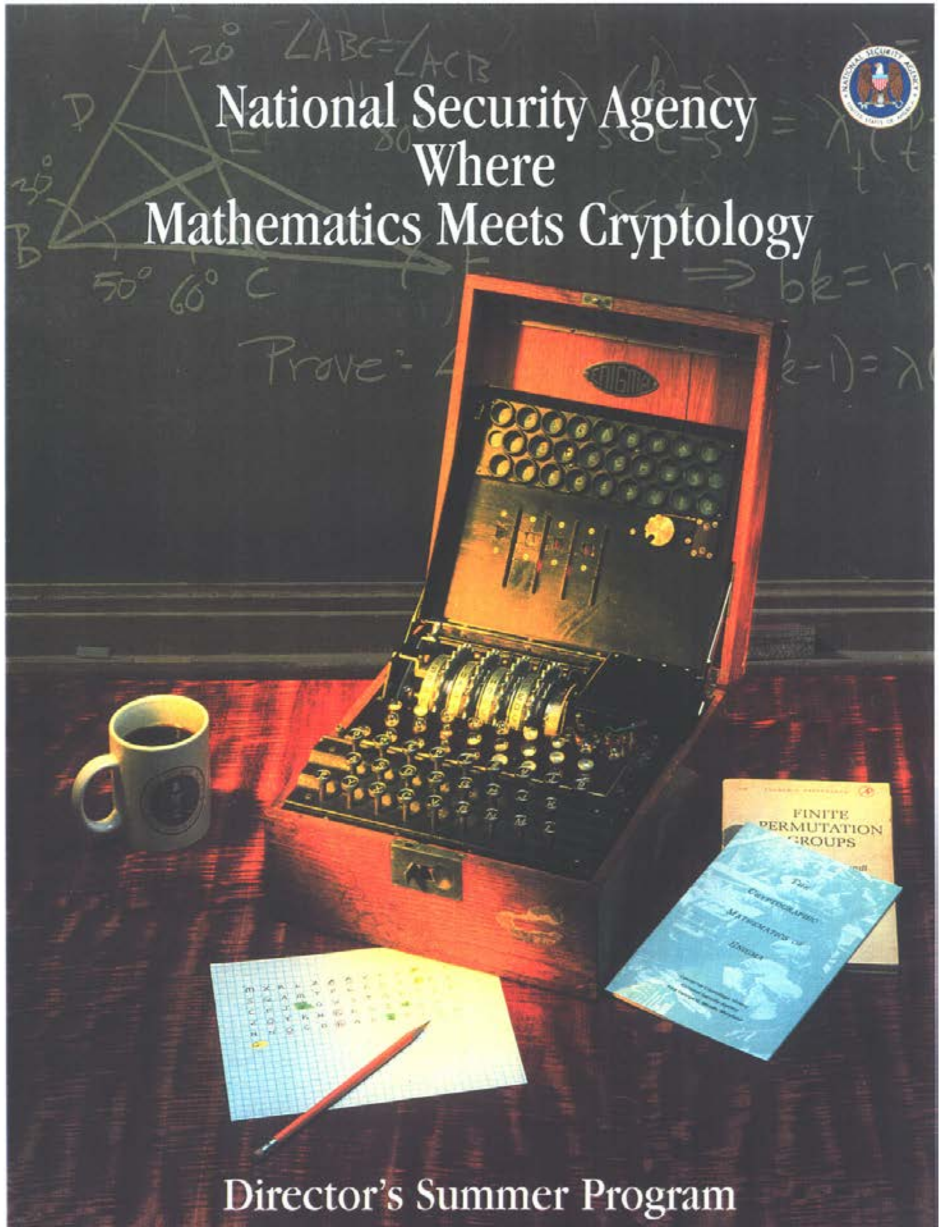
The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

Section III proposes two approaches to transmitting keying information over public (i.e., insecure) channels without compromising the security of the system. In a *public key cryptosystem* enciphering and deciphering are governed by distinct keys, E and D, such that computing D from E is computationally infeasible (e.g., requiring 10^{100} instructions). The enciphering key E can thus be publicly disclosed without compromising the deciphering key D. Each user of the network can, therefore, place his enciphering key in a public directory. This enables any user of the system to send a message to any other user enci-

The manifesto

- Key distribution as the central problem for enabling e-commerce
- Public-key (asymmetric) crypto as the solution to decentralized trust
- Crypto is recast as an open mathematical problem space
  - “At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.”
- Break from Cold War “secrecy through obscurity” paradigm –
  - Civilian research, publication, peer review
- And signatures!

National Security Agency
Where
Mathematics Meets Cryptology


∠ABC=∠ACB
Prove:
ENIGMA
FINITE PERMUTATION GROUPS
The Cryptographic Mathematics of Enigma

Director's Summer Program

WIRED

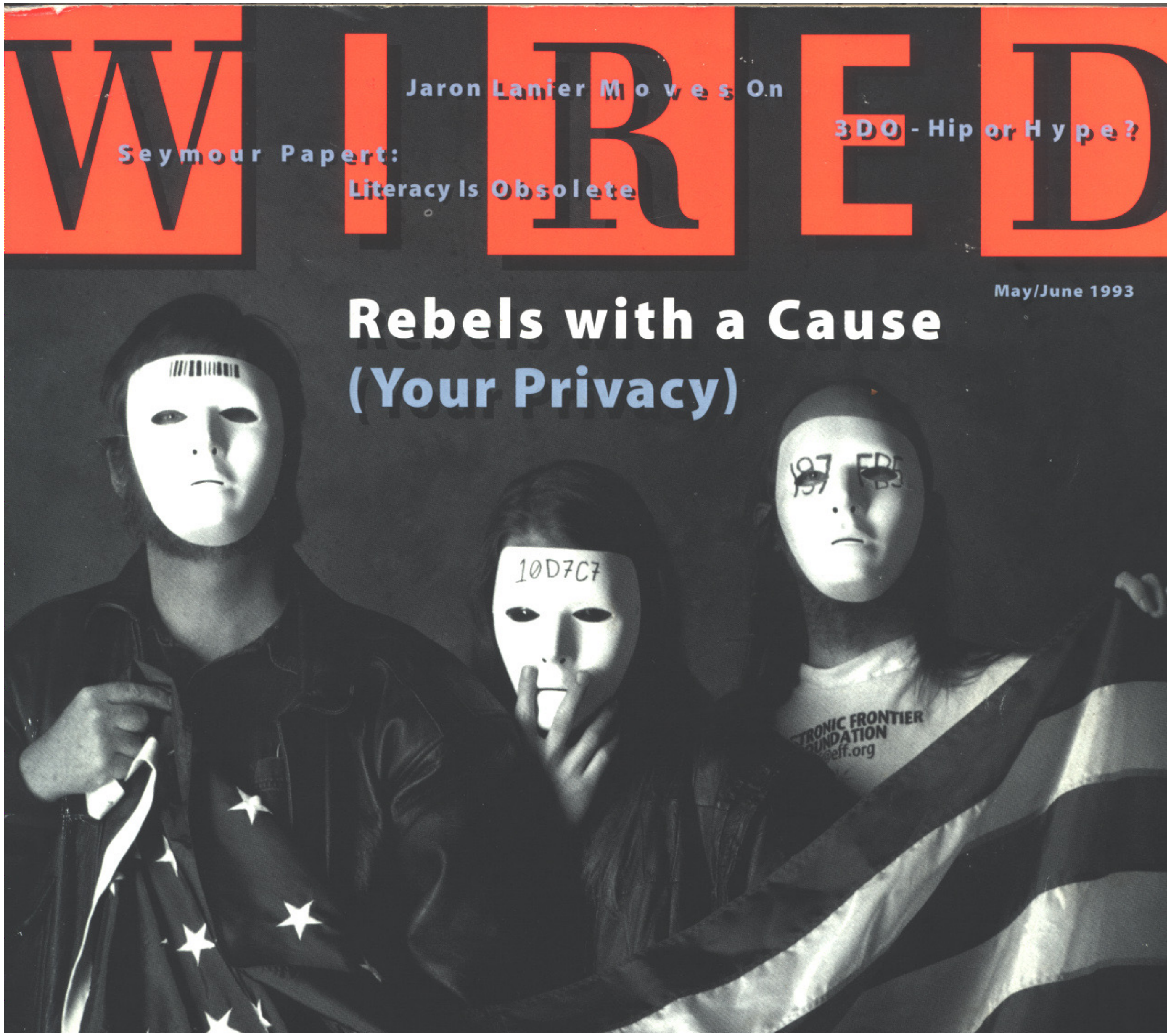
Jaron Lanier Moves On

3DO - Hip or Hype?

Seymour Papert:
Literacy Is Obsolete

May/June 1993

Rebels with a Cause (Your Privacy)



GREENSPAN'S GAMBLE: CAN RATE CUTS STAVE OFF A SLUMP?

Newsweek®

January 15, 2001

newsweek.msnbc.com

Beating Big Brother

EXCLUSIVE BOOK EXCERPT

How Computer Rebels Kept the Government From Spying on You

By Steven Levy

Foundational programs

- Crypto-anarchists:

  Crypto as *liberation technology*; decentralization, resistance to surveillance, and trust without institutions.

- Chaum:

  Privacy as a *design mandate*; new primitives (blind signatures, digital pseudonyms) to reorganize social relations.

- Simmons:

  Cryptography as tasked with reproducing the locks and chains of paper-based security in a digital environment.

- Goldreich:

  Cryptography anchored in mathematical rigor—proofs, formal models, and adversaries abstracted from the world.

Emergence of the signature model

- Diffie & Hellman (1976): foundational metaphors
  - “In order to develop a system capable of replacing the current written contract with some purely electronic form of communication, we must discover a digital phenomenon with the same properties as a written signature.”
  - “It must be easy for anyone to recognize the signature as authentic, but impossible for anyone other than the legitimate signer to produce it. We will call any such technique one-way authentication.”
- The RSA paper intensifies abstraction
  - Defines signatures as an inversion of encryption, without engagement with legal or evidentiary traditions.
  - Uses scare quotes: “Therefore Alice has received a message ‘signed’ by Bob, which she can ’prove’ that he sent, but which she cannot modify.”
- The core design brief is modeled on *function*, not *context*.

New kinds of signatures

- Blind signatures
  - Signer does not see the content they sign.
  - Developed by Chaum for digital cash and anonymous credentials.
- Undeniable signatures
  - Cannot be verified without the signer’s cooperation.
  - Interactive proof rather than public verifiability
- Group signatures
  - A member (or coallition) of a group can sign anonymously on behalf of the group.
  - New creative arrangement of authentication and anonymity.
- Proxy signatures
  - Delegate signature authority from one party to another.
  - Enables controlled delegation without exposing the original signer’s private key; both parties remain accountable.

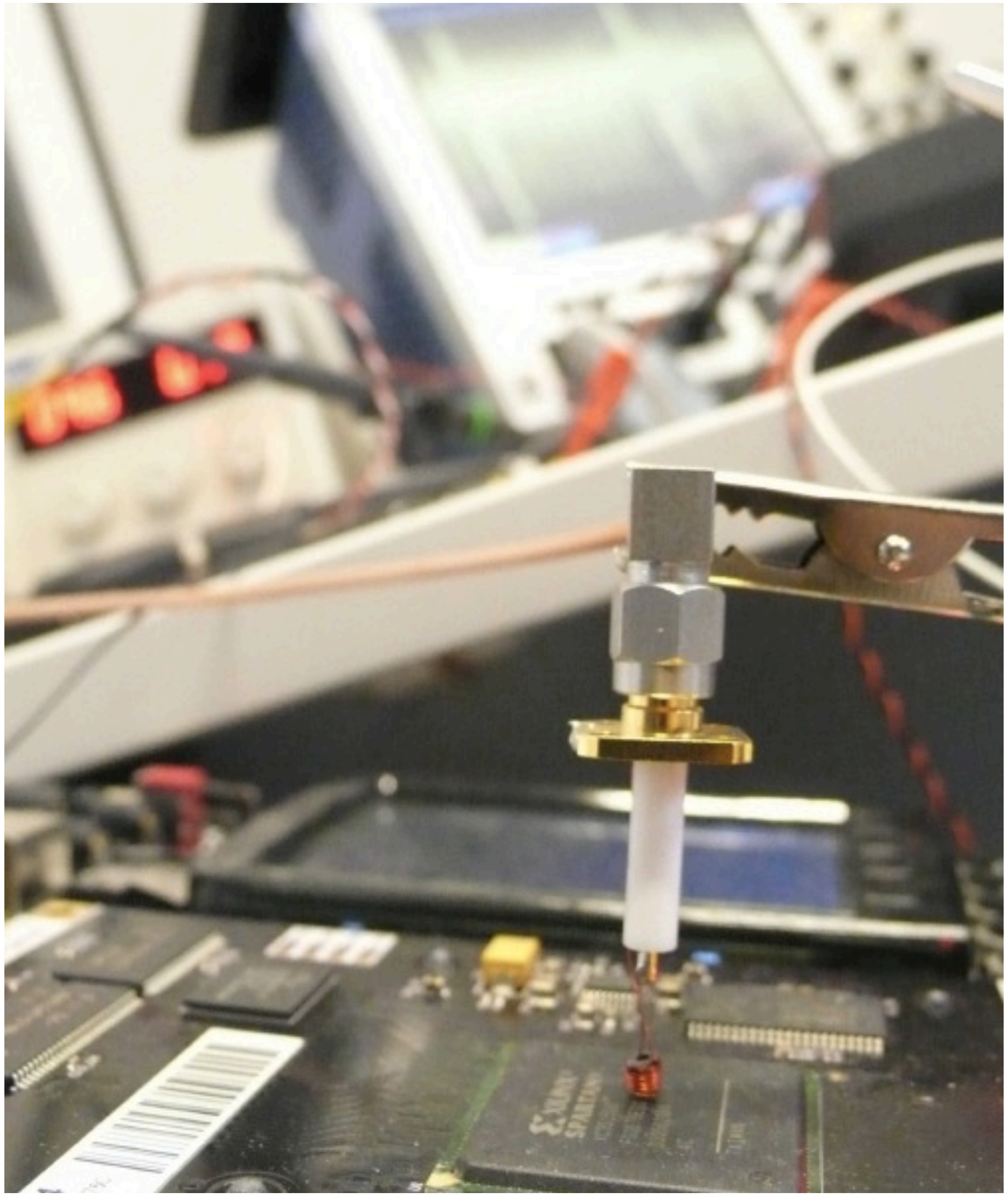
Justificatory scenarios

- “Suppose that Bob (also known as “Deep Throat”) is a member of the cabinet of Lower Kryptonia, and that Bob wishes to leak a juicy fact to a journalist about the escapades of the Prime Minister in such a way toat Bob remains anonymous, yet such that the journalist is convinced that the leak was indeed from a cabinet member. Bob cannot send a standard digitally signed message, since such a message, although it convices the journalist that it came from a cabinet member, does so by directly revealing Bob’s indentity.”

IN THE KINGDOM OF LOWER KRYPTONIA— A SMALL BALKAN STATE ...
THERE IS DISSENSION IN THE CABINET, GENTLEMEN...
ONE OF US CANNOT BE TRUSTED.
BOB—CECETTLY KNOWN AS "DEEP THROAT"—IS TROUBLED...
IT IS ONLY A MATTER OF TIME BEFORE THEY TURN ON!
I HAVE INFORMATION FOR YOU, BUT I MUST REMAIN ANONYMOUS.
YES—YOUR SECRET IS SAFE WITH ME!

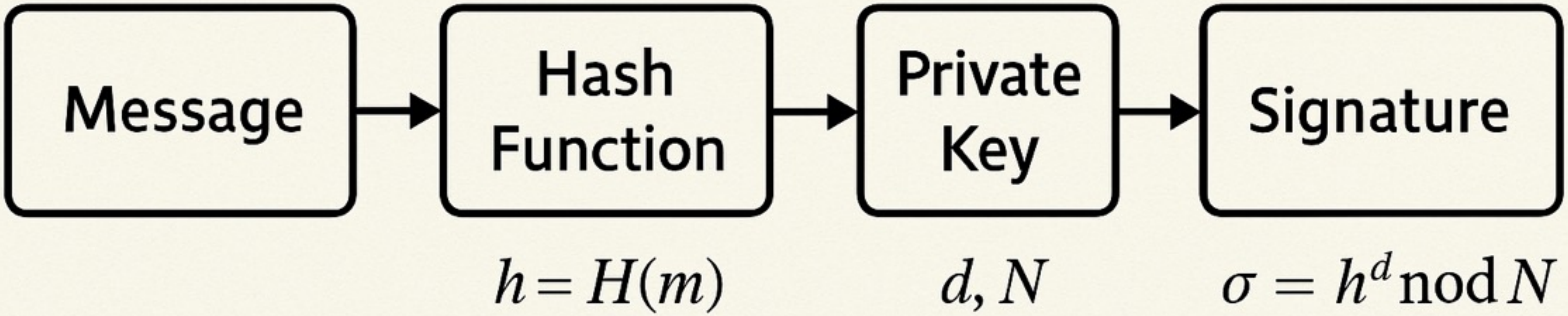
Internal criteria, external relevance

- Cryptographic signatures were not defined by empirical needs, user demand, or institutional practice, but by what could be formalized and proven.
- Once formalized, schemes are evaluated by internal criteria (e.g. security proofs, efficiency), not external relevance.
- The design mandate of cryptography comes not from the world, but from within the discipline itself — its assumptions, its models, its aesthetics, its needs for mathematical rigor, couched by Goldreich as ‘natural security concerns’
- Even worse: this does not account for the creative activity of cryptographers, the entirely new objects they create, resulting in the over-extended justificatory scenarios.



Side-Channel Attacks

- Involuntary steganographic leaks
- Major crack in the 'standard model'
- The model has formalized away that computation is always material
- Unlike Turing Machines, computers consume energy, emit radiation, etc.



Message

Hash Function

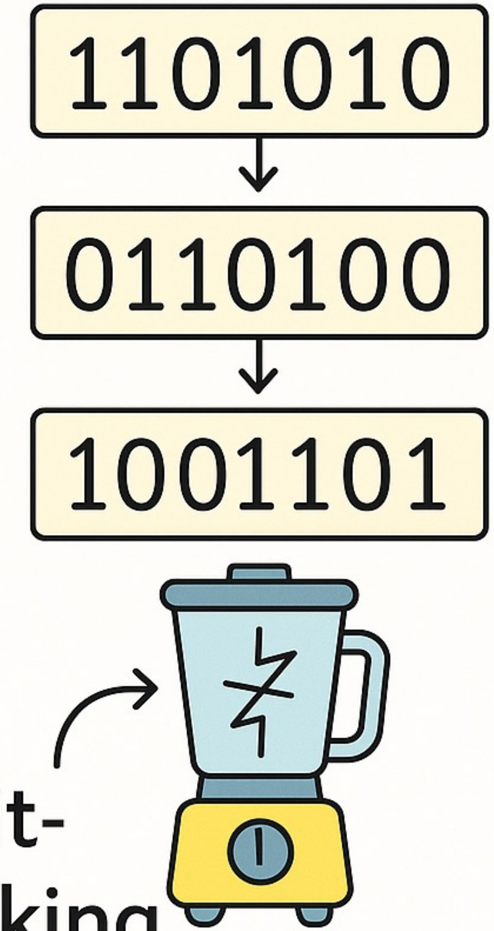
Private Key

Signature

$h = H(m)$

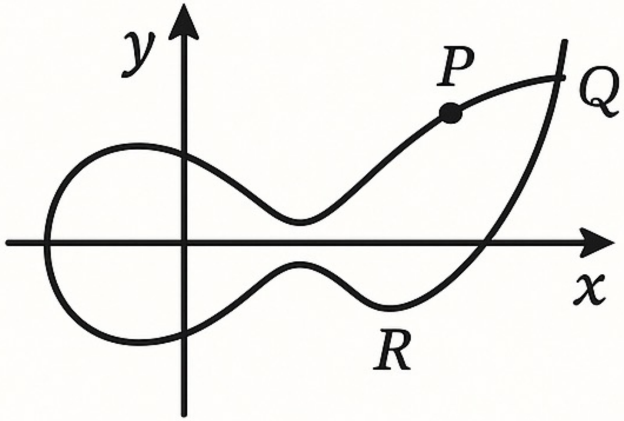
d, N

$\sigma = h^d \operatorname{nod} N$



Bit-shaking algorithms

$$a^b \bmod p$$



Number-theoretic algorithms

Random oracle model controversy

- In the 90s, a series of protocols proved secure in theory turned out to be insecure in practice.
- Bellare and Rogaway (1993) seek a bridge between theoretical security and practical construction.
- ROM: A hash function is idealized as a “random oracle”: a black box that outputs a truly random value for each unique input.
- **BUT:** No real hash function behaves like a random oracle.
  The model is powerful but epistemically unstable.
- **BUT:** Allows formal proofs for practical protocols:
  - “This is the only way we know how to prove RSA signatures secure.”
  - “We stress that the last step of the proof is heuristic in nature. … Significant assurance benefits nonetheless remain.”

Strong words are exchanged …

- Goldreich: this is “post-modern” cryptography:
  - ROM-based proofs are built on an idealization that is impossible to instantiate.
  - There exist schemes that are secure in the ROM and insecure under all real hash functions
  - Intellectually lazy and methodologically weak.
- ROM remains widely used: it is efficient, intuitive, and the only tractable option for many constructions.
- The controversy puts another crack in the “standard model”:
  - Rogaway: “When you are working with the ROM, you are working within a specific model, and a not-so-realistic one at that. What is often not recognized is that when you are working within the standard model, you are *also* working within a specific model and a not-so-realistic one. The standard model *also* abstracts away key aspects of the real world—like the fact that real computation takes time, uses power, and leaks radiation. There *is* a big gap between the ROM and reality (hash functions *aren’t* like random oracles) — and there is *also* a big gap between the standard model and reality.”
- Security proofs are always contingent on *some* abstraction — at least, ROM is upfront about its assumptions.

And so? …

- Cryptographers claim a libertarian ethos, yet rely on an authoritarian model of proof (Goldreich).
- In practice: multiple proof regimes coexist — ROM, “standard” assumptions (RSA is hard), and communal evidence that schemes remain unbroken.
- If cryptographic proofs already draw on diverse and imperfect foundations, why not develop modes of proof shaped by the realities of institutions, users, and practice?
- This is about opening and exploring the space of design

Memory

```
0. _ _ _ _ _ _ _ _
1. t _ _ _ _ _ _ _
2. t o _ _ _ _ _ _
3. t o m _ _ _ _ _
4. t o m a _ _ _ _
5. t o m a t _ _ _
6. t o m a t o _ _
```

(a) Left-to-right

```
0. _ _ _ _ _ _ _ _
1. _ _ _ _ _ _ _ t
2. o _ _ _ _ _ _ t
3. o m _ _ _ _ _ t
4. o m a _ _ _ _ t
5. o m a t _ _ _ t
6. o m a t o _ _ t
```

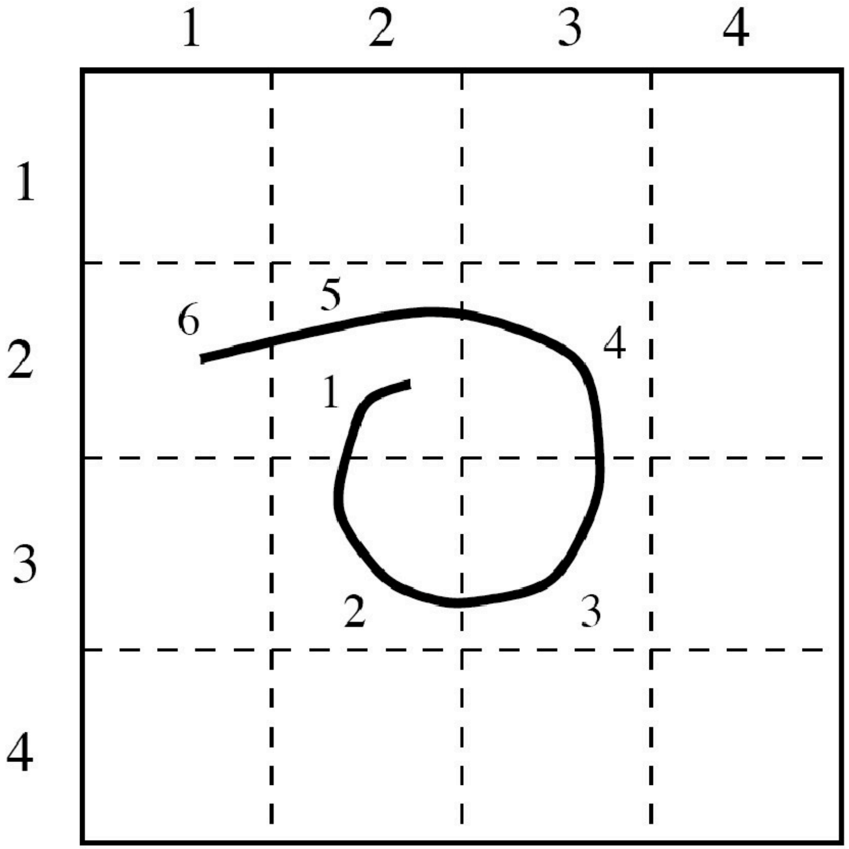
(b) Rotated left

```
0. _ _ _ _ _ _ _ _
1. t _ _ _ _ _ _ _
2. t _ _ _ _ o _ _
3. t m _ _ _ o _ _
4. t m _ _ a o _ _
5. t m t _ a o _ _
6. t m t o a o _ _
```

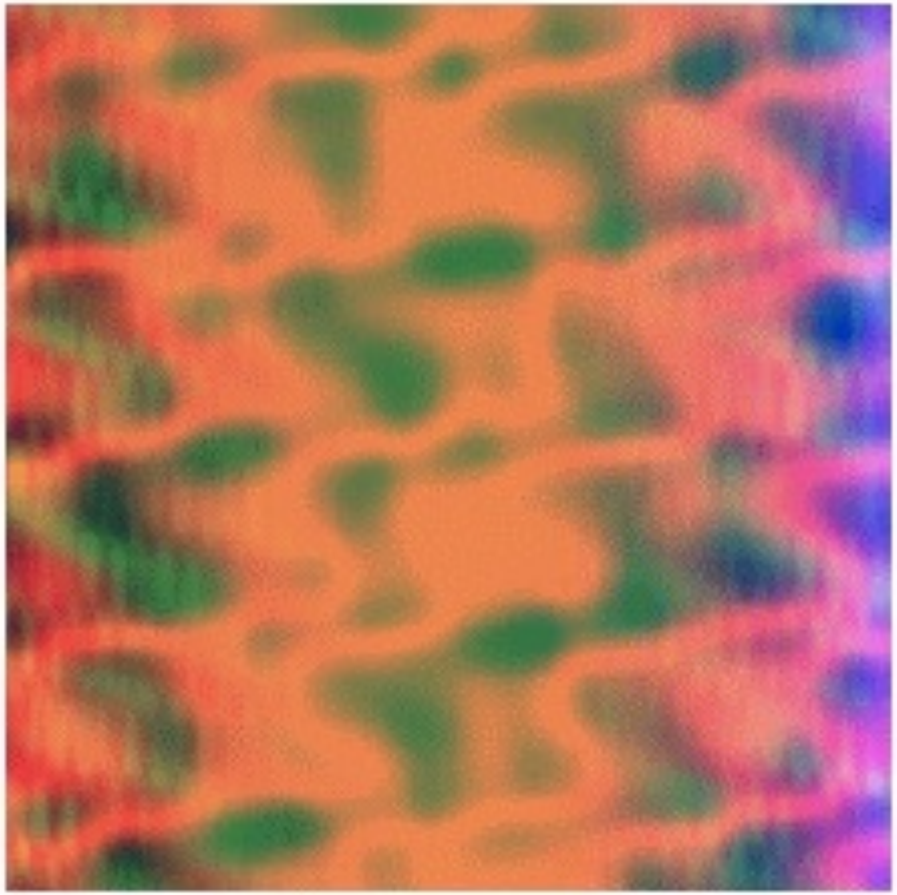
(c) Outside-in

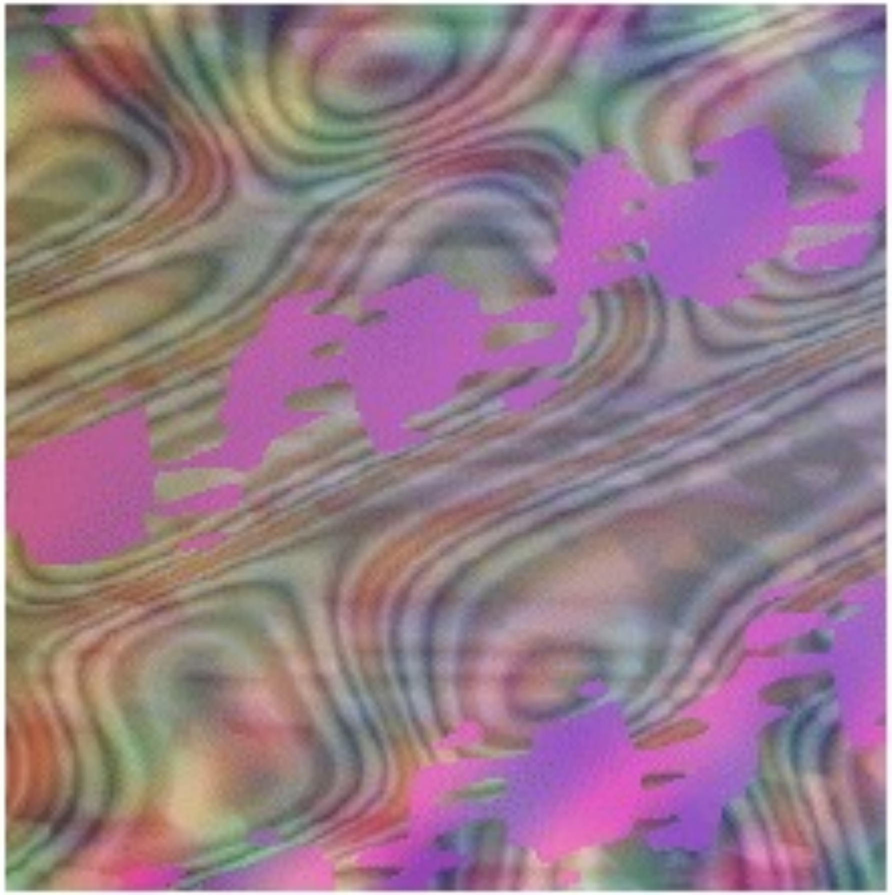
```
0. _ _ _ _ _ _ _ _
1. _ _ _ _ _ _ _ t
2. _ _ _ _ o _ _ t
3. m _ _ _ o _ _ t
4. m _ _ a o _ _ t
5. m t _ a o _ _ t
6. m t o a o _ _ t
```

(d) A more complex example



Visual system (hash visualization)



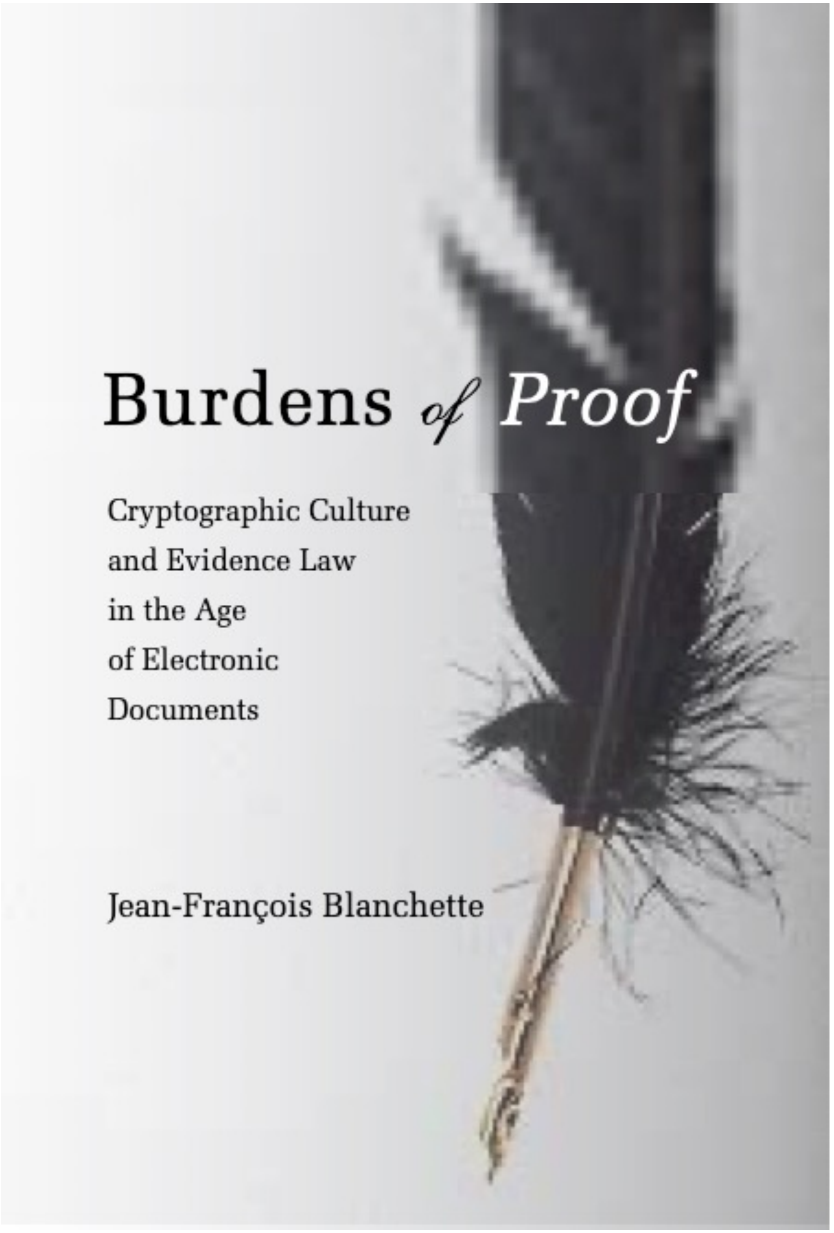


Embodiement & materiality as inspiration

- Memory
  - Schemes that rely on input orderings, recognition, and unshareable secrets
  - Leverage subjective, non-transferable memory rather than shared secrets or public keys
- Vision
  - Graphical passwords, hash visualizations, and visual cryptography
  - Embed authentication in perception, what can be seen, not just computed; invoke intuitive pattern recognition
- Cognition
  - Unplugged crypto, KidKrypto — make cryptographic reasoning mentally executable, not just machine-verifiable
- Material objects
  - Sealed envelopes, scratch cards, tamper-evident seals
  - Anchor cryptographic guarantees not digital abstraction, but in physical irreversibility and tactile inspection

Conclusion

- Cryptography arrived on the scence of digital evidence with grand ambitions, but the end results have been less than spectacular
- Law translated and domesticated cryptographic claims rather than adopting them wholesale.
- Legal professions and archives reasserted their own regimes of trust, with limited interest in cryptography’s authority.
- Cryptography’s own trust practices are more diverse, more creative, more pragmatic than it likes to admit.
- Cryptography’s relevance might be improved by broadening its modes of proof, engaging with the social and material world, and embracing a culture of speculative design experiments



Burdens of *Proof*

Cryptographic Culture
and Evidence Law
in the Age
of Electronic
Documents

Jean-François Blanchette