


Pay TV



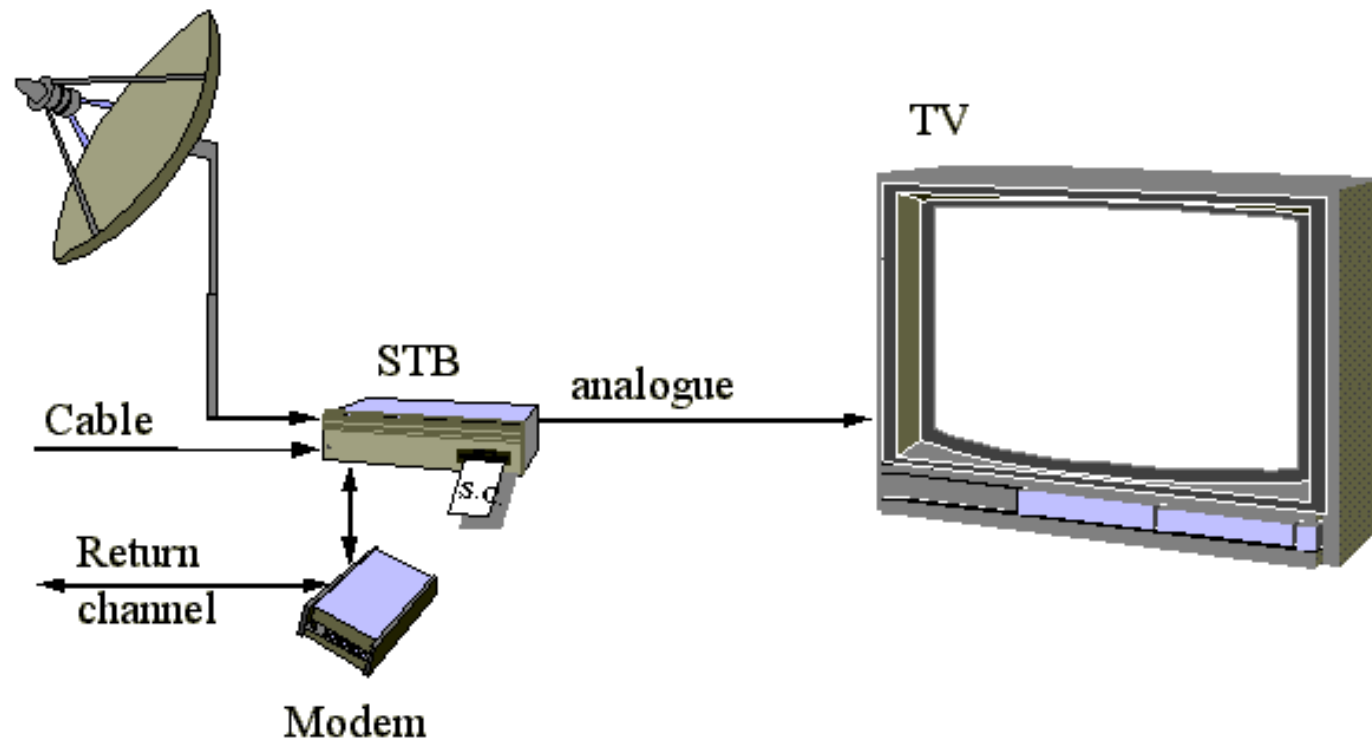
Nicolas T. Courtois^{1,ex. 2}

¹  - University College of London, UK

²  = [Axalto+Gemplus]
security to be free



Pay-TV



Bottom Line

The problems of:

- Protecting Pay TV from piracy
- A DVD movie / CD songs from copying
- Microsoft Windows from copying
- Console games, etc.
- Bank cards from fraud
- Building passes / London Oyster card from cloning

Have ALL essentially two solutions:

- always online solutions (e.g. online activation, online authorization etc]
- solutions based on 'unclonable' hardware tokens such as smart cards.

Moreover none of these two techniques is perfect in isolation. The future is about combining both online + smart cards solutions.

Hacking PayTV

(not for print)

Low-level Attack

- Beer glass icon in pubs [Sky sport channels]
 - one can buy a sticker on ebay!

Famous Hacker

Christopher Tarnovsky



Tarnovsky Testimonial Against NDS

"Sure, I've broken the cards of Kudelski",

"I was paid by NDS to do it. This is an activity that all companies in the trade do."

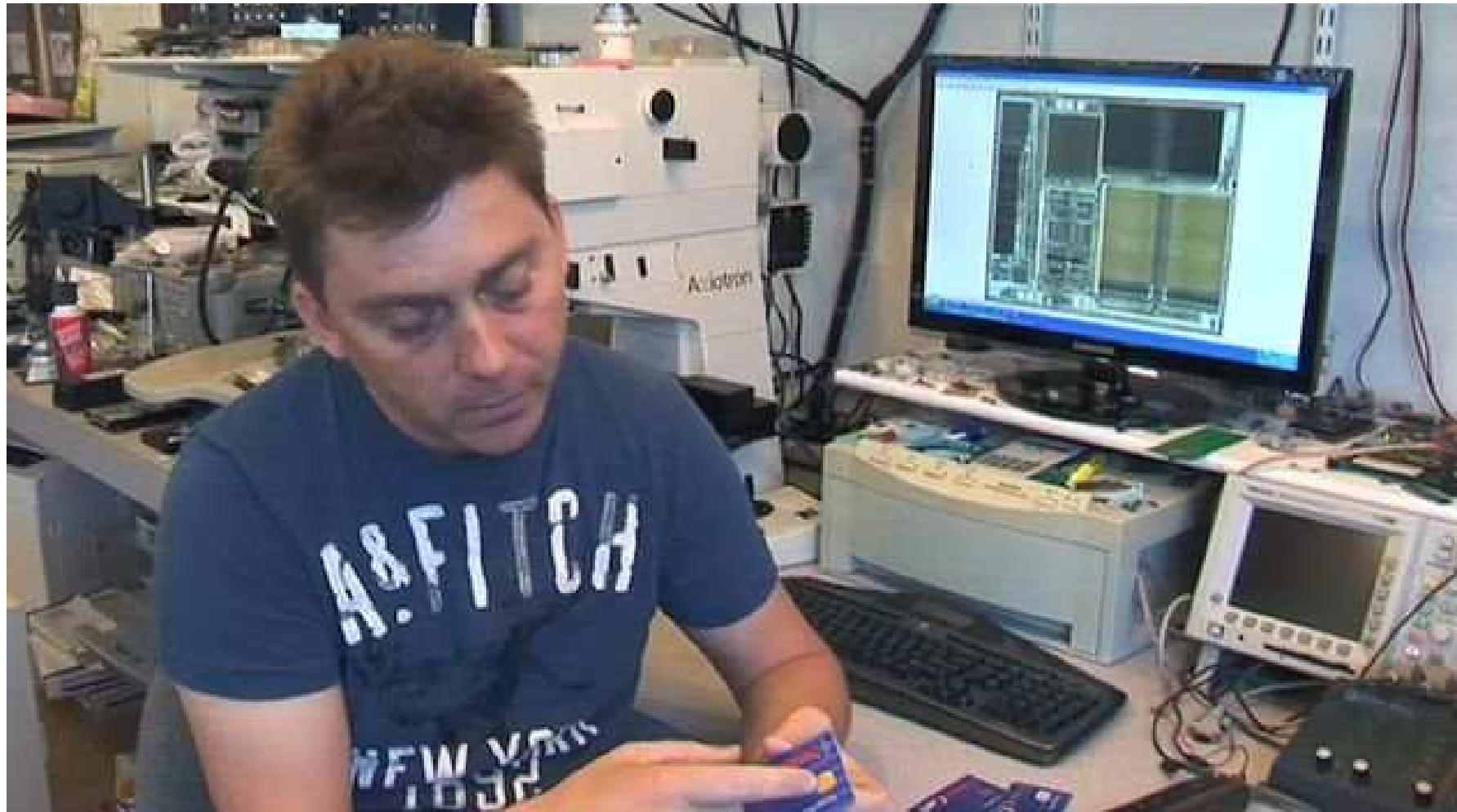


He also said that he was offered 100 000 dollars if he can break Xbox360. He replied that it was not enough.

Silicon Hacking

Tarnovsky Lab

Only few thousands of dollars of equipment



Tarnovsky (and Other Professional Chip Hackers)

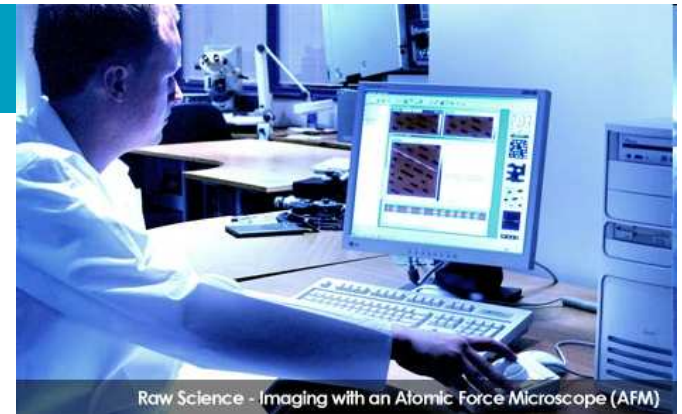
Few thousands of dollars of equipment

- Surface polishing
- HydroBromic acid to eat away the passivation layers
- A microscope for pictures:
 - the successive layers of silicon are revealed with acids and lasers
- Doping guns to cut/add traces to a working IC
- Stinger: bypassing the protections with long microscopic needles.

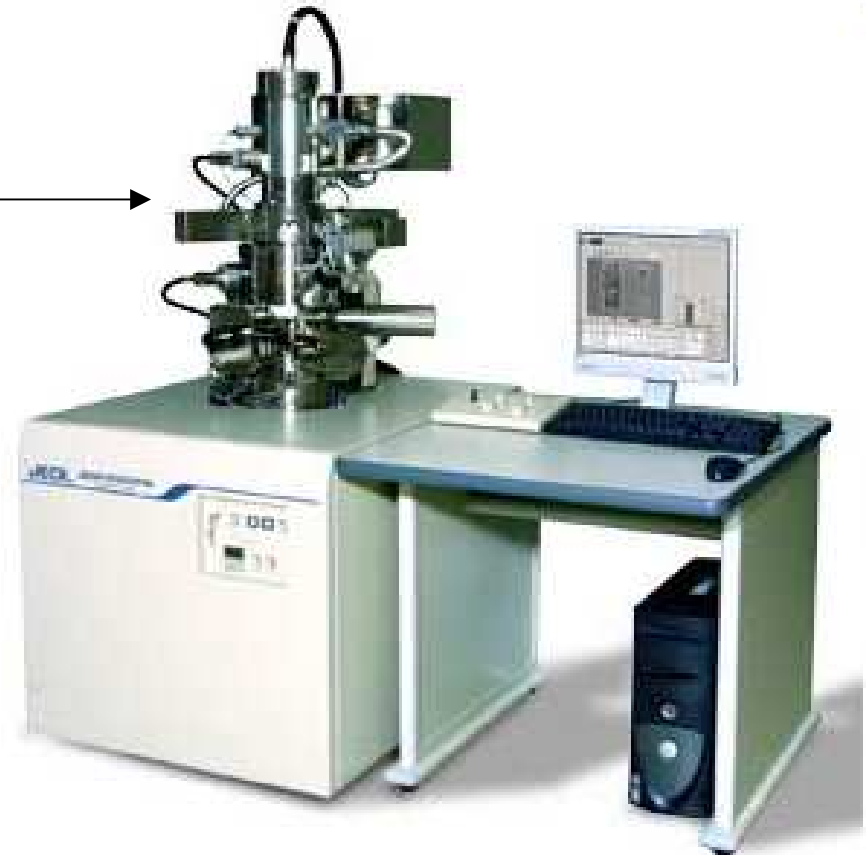


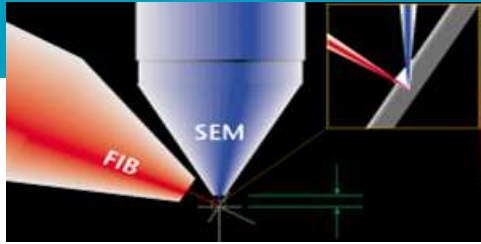
More Expensive:

- Atomic Force Microscope



- FIB device
(Focused Ion Beam, 0.5 M€)
Canal+ Technologies Lab





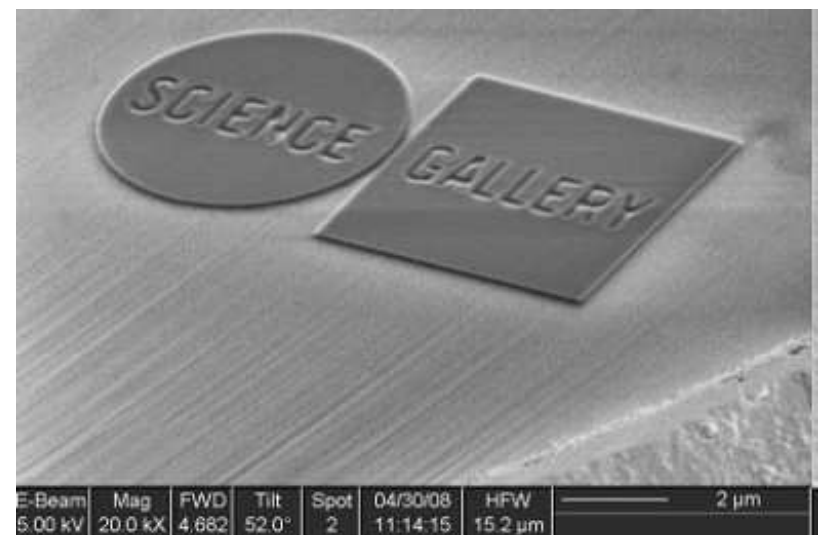
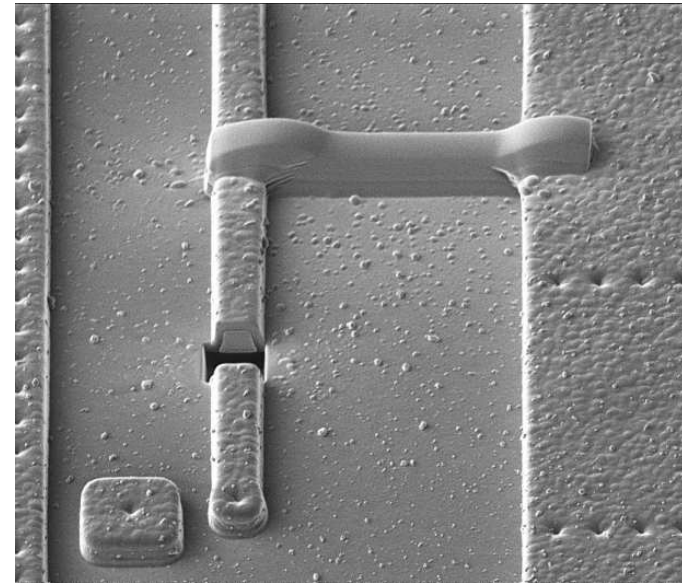
FIB:

Example resolution: 10 nm

Classical applications: failure analysis of ICC

But also: circuit modification:

- Local material removal:
 - cutting metal lines, milling, gas enhanced etching
- Local rebuilding/rewiring of the device
 - new metal interconnects
 - new insulating layers
- Fine tuning of analog components: decrease/increase R or C...
- Reading (electron image) ←
- Art: writing on the nm scale: →



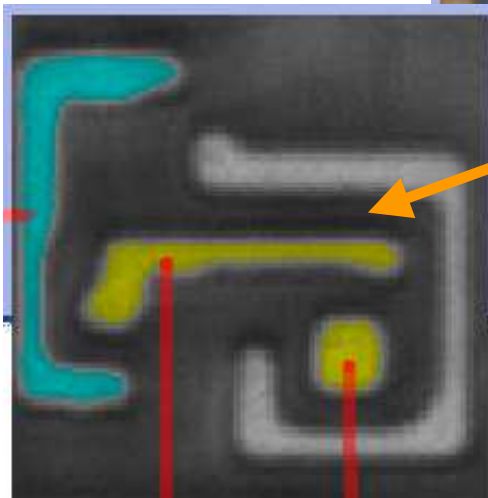
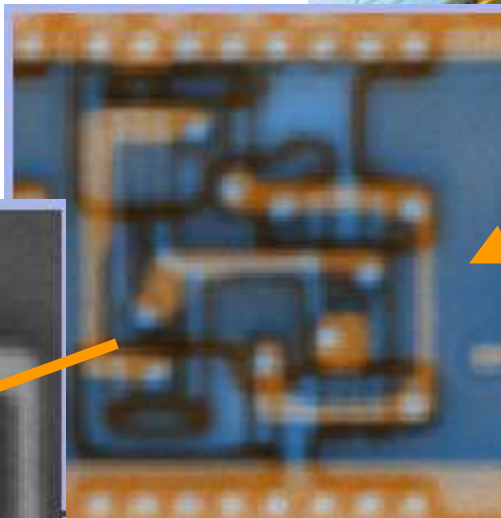
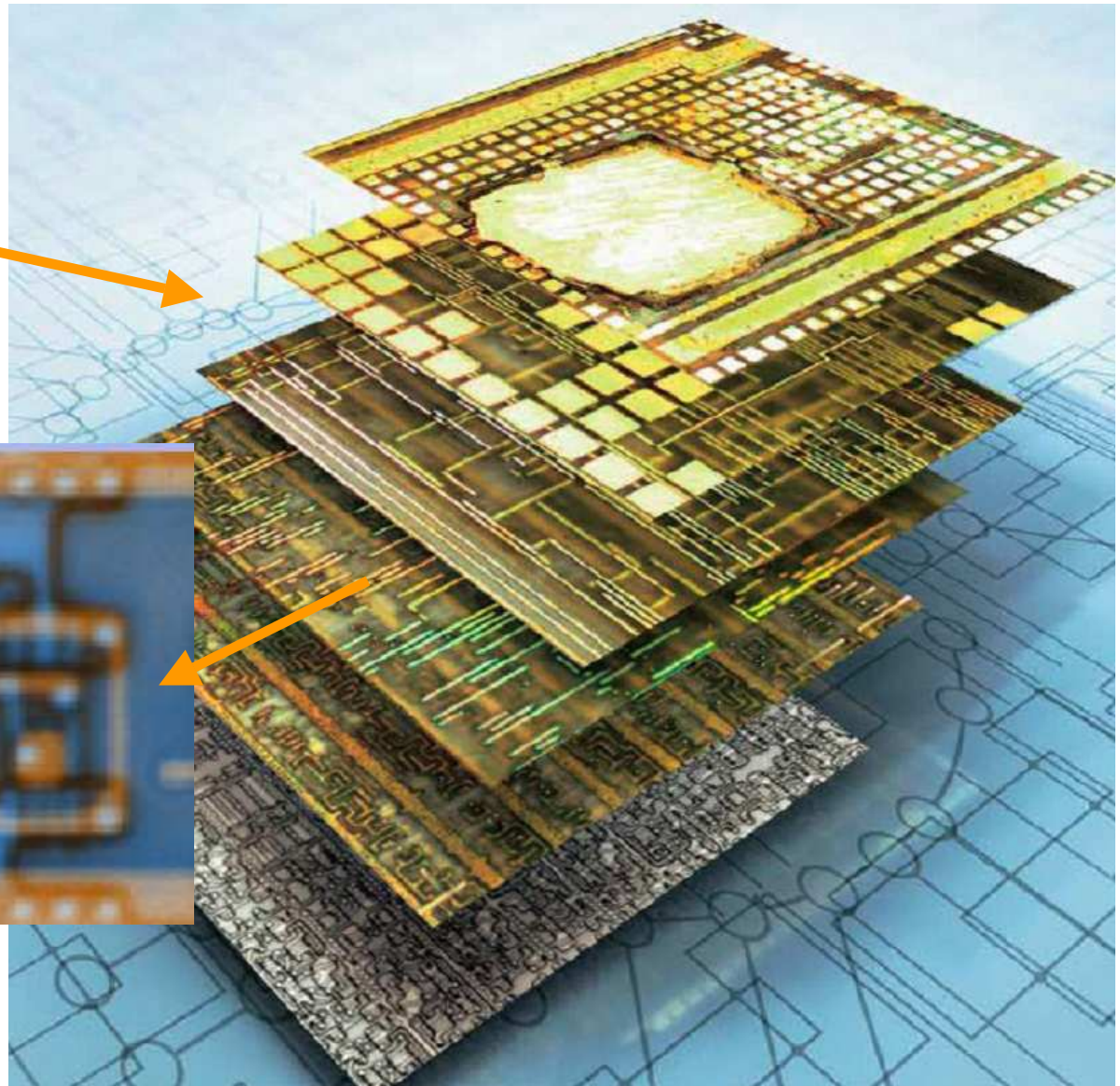
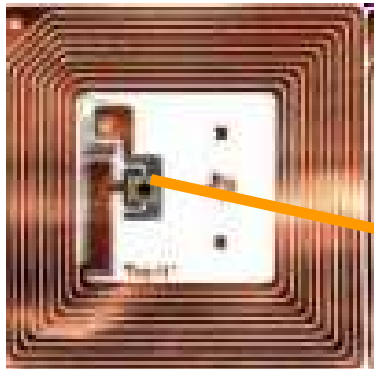
Clear and Present Danger

Reverse engineering is NOT that hard.

No no need for a FIB device
(Focused Ion Beam, 0.5 M€).

A few thousand dollars microscope will suffice.

Reverse Engineering MiFare [Nohl, Plotz, 2007]



is 2008

Open Source vs. Closed Source Crypto

(VERY important issues in PayTV)

Kerckhoffs Principle

Dutch cryptologist, wrote his book in French.

In June 2006 Dutch researchers De Gans et al, have published several cloning attacks on MiFare Classic chips [London Oyster card + 200 M other].

[first cloning attack: Courtois, Nohl and O'Neil, April 2008].

Kerckhoffs principle: [1883]

“The system must remain secure should it fall in enemy hands ...”



Remark

Smart Cards:

They are already in ‘enemy’ hands



Kerckhoffs principle: [1883]

Most of the time: incorrectly understood.

Dutch researchers

No obligation to disclose.

- Security when disclosed.
- Better security when not disclosed.

Kerckhoffs principle is **WRONG**
in the world of secure hardware devices

Dutch researchers got a large grant to develop an OPEN SOURCE replacement for the Oyster card system.

This cannot work.

- Algorithm secrecy [once they are good] **MUST** be preserved.
- Reason: side channel attacks are **VERY** hard to prevent.
- More reasons in Pay TV.

Kerckhoffs principle is WRONG

- In Pay TV [traditional like satellite broadcast] there is no need to recover the key. It is transmitted to too many parties and can be extracted from another decoder and broadcasted to other people.
- So as soon as the algorithm is public, the key can be diffused and everybody will watch the content.
- The algorithm must remain secret.

Custom Crypto

Case Studies

- PayTV: algorithms were updated hundreds of times, systems were cracked as soon as the algorithm was reverse engineered.
- In GSM/3G:
 - the encryption algorithms are public
 - broken for all 2G algorithms.
 - The authentication algorithms [protect the operator's \$\$\$] are SECRET and were NEVER hacked so far.
- In bank cards, all algorithms are public.

Yet there was no hacker attack on them yet
[many other attacks are easier as of yet!]

Custom Crypto: Our Two Patents [Courtois et al. Gemalto]



76.0 – PAIRING – A UNIVERSAL CRYPTOGRAPHIC MODULE

CONTEXT

New generic cryptographic solution to secure the communication between devices.

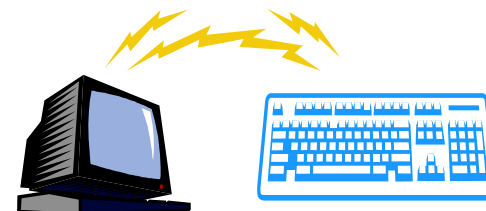
INVENTION

The invention consists of providing two (or more) identical cryptographic modules embedding identical cryptographic algorithm and key, allowing a secure point to point connection when inserted in two communicating devices. There is no necessity (and no possibility) for said devices of key generation or key management. The modules are manufactured/ distributed/sold/ installed by two, and may be replaced, at any moment, by a new couple of modules.

APPLICATIONS (not exhaustive)

Wireless point to point connections: Bluetooth headsets, wireless keyboard/mouse, secure WiFi, wireless USB, TV remote, pay-TV,...

Access Control: car key/beeper, detachable-face car radio, contactless keys for hotel room, PC login tokens, ...



Application:

Pay per view pay TV without any broadcast channel. Assume that broadband wireless Internet is a commodity [it already is in the UK, 5£/month].

- Just buy a SIM card from a local shop.
 - Connect wirelessly to this local shop.
 - Private channel.
 - Can be used also in an airport or hotel.
 - Highest possible security: in each card pair the crypto algorithm etc.. can be different.
 - 0 % piracy is possible.

Another Patent

- Nicolas Courtois and Louis Goubin, Gemalto]
- A machine for automatic generation of custom crypto algorithms.
- Great variability, locally look like random CPU instructions (!).
- Makes it possible to have a different algorithm in each smart card, in flash memory, updated over the net.
 - Future of PayTV/console games/software protection security?

PayTV Business Analysis

Two Markets of TV

- Mainstream TV:

- Goal: Acquiring/Capturing the attention of the public on behalf of government and advertising companies.
- Content is freely available (no technical obligation to pay).

- Pay TV:

- Opposite goal: Selling the content to the public.
- Content is scrambled / encrypted.

**Financing the TV

- **Mainstream TV:** (state -> privately owned)

Pay for the 1) public attention acquired. 2) the content

- Public TV: financed by

- Special tax (redevance audiovisuelle) and
- Advertising.

- Private TV:

- Advertising (TF1, M6).

- **Pay TV:** (privately owned), pay for 1) the content 2) the public:

- Financed by

- Subscription
- Advertising

Broadcasting Technology

- Mainstream TV:

- UHF/VHF national coverage
- Complemented by cable and satellite (remote areas)

- Pay TV:

- Satellite (out of date, declining everywhere)
- Cable (stagnating in Europe DVB-C, growth in the US – Comcast instead of DSL)
- New: DSL (Freebox, France Télécom TPS-L)
- DVB-T (numérique terrestre – TNT), in France since April 2005.
- DVB-H, mobile phone services...

*Economic Models of Pay TV:

- **Pay per view** (several types): (5 % of the market)
 - Video-on-Demand Movie Channels
 - Video-on-Demand XXX
 - Niche markets: Hotels
 - Prepaid cards for 1 year.
 - XXX
- Main: Channel Subscription
 - Monthly subscription for one or several channels.

Essential (Historical) Limitation:

- **One-directional** channel, no return channel.
 - UHF/VHF
 - Satellite until very recently.
 - Cable TV before 1996-2000.
- Heavy Bandwidth Limitations.
- The same signal is sent to everyone. (unidirectional – descendant)
 - Limited possibility of multiplexed access (again bandwidth pb.).

⇒ **BROADCAST ENCRYPTION / CHANNEL**

- Similar issues: protecting DVD from copying, also pay for online database.

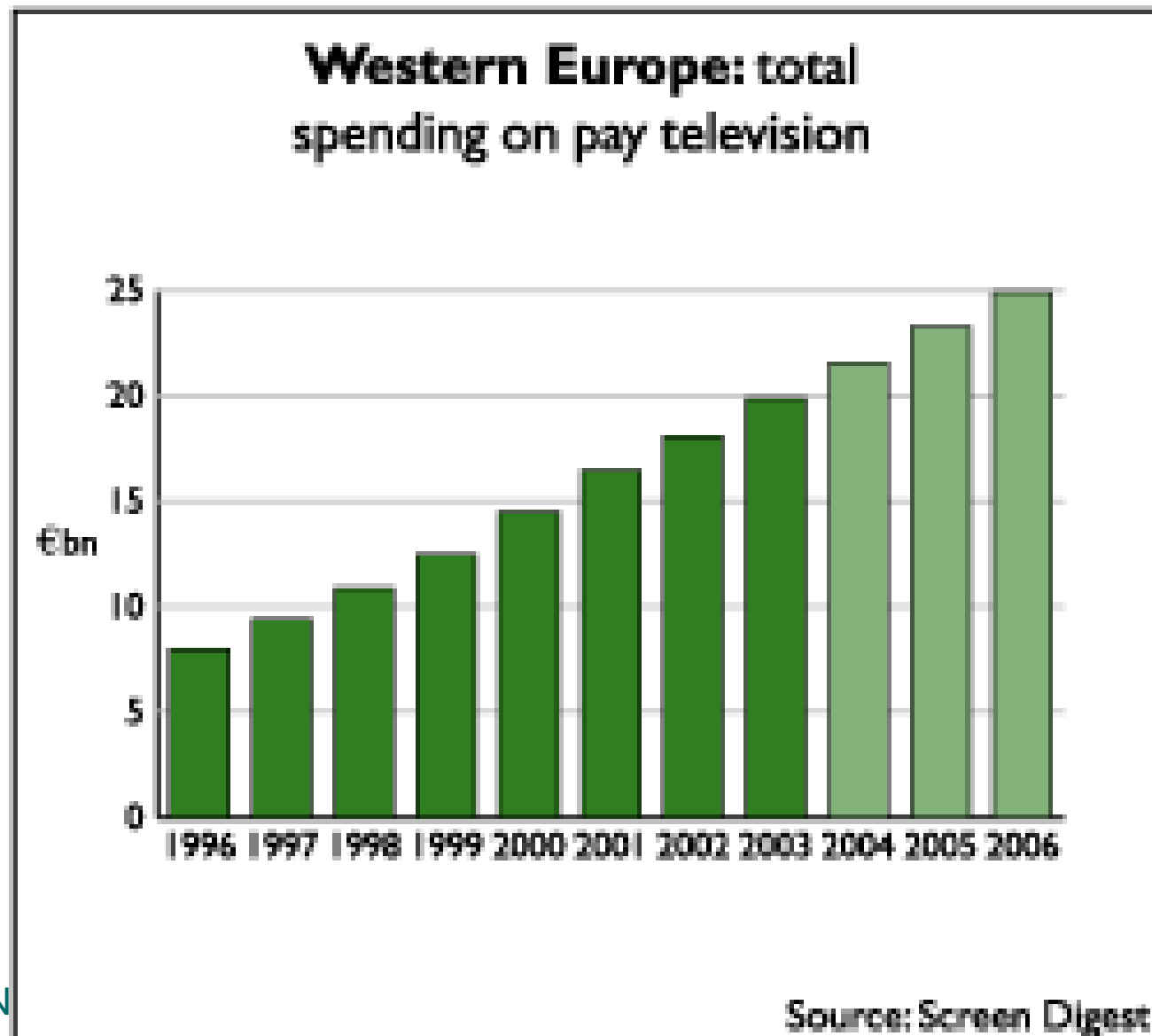
Prospects of Pay-TV

- General Decline of TV in the 1990s (- 1 million in France)
 - Loss of relative interest: Budget and attention captured by GSM, Video games, PC, laptop and handheld.
- Technical Decline of Current Pay TV Technologies: today:
 - Existing broadcast encryption still used...
Satellite advantages are out of date compared to Cable/DSL/Internet.. Except in remote areas !
 - Increasingly we have the backwards channel:
 - New Pay-TV technologies: : - 2000s:

Technically: General e-commerce of immaterial goods (e.g. software).

- BUT: will not go this way, owners of the content will not allow it.
- No security, revenue loss if open systems/software.

Decline of Pay-TV ?



Prospects of Pay-TV - Europe

Source: www.screendigest.com

- > 20 Billion € in 2004 in Europe.
- Penetration: 50 per cent in 2004.
 - Mostly analogue pay TV.
- Digital PayTV: exponential growth.
- In real terms, the year-on-year growth in ARPU has been falling throughout Europe across all delivery platforms.

Necessary Ingredients for Pay-TV

For all types of Pay-TV:

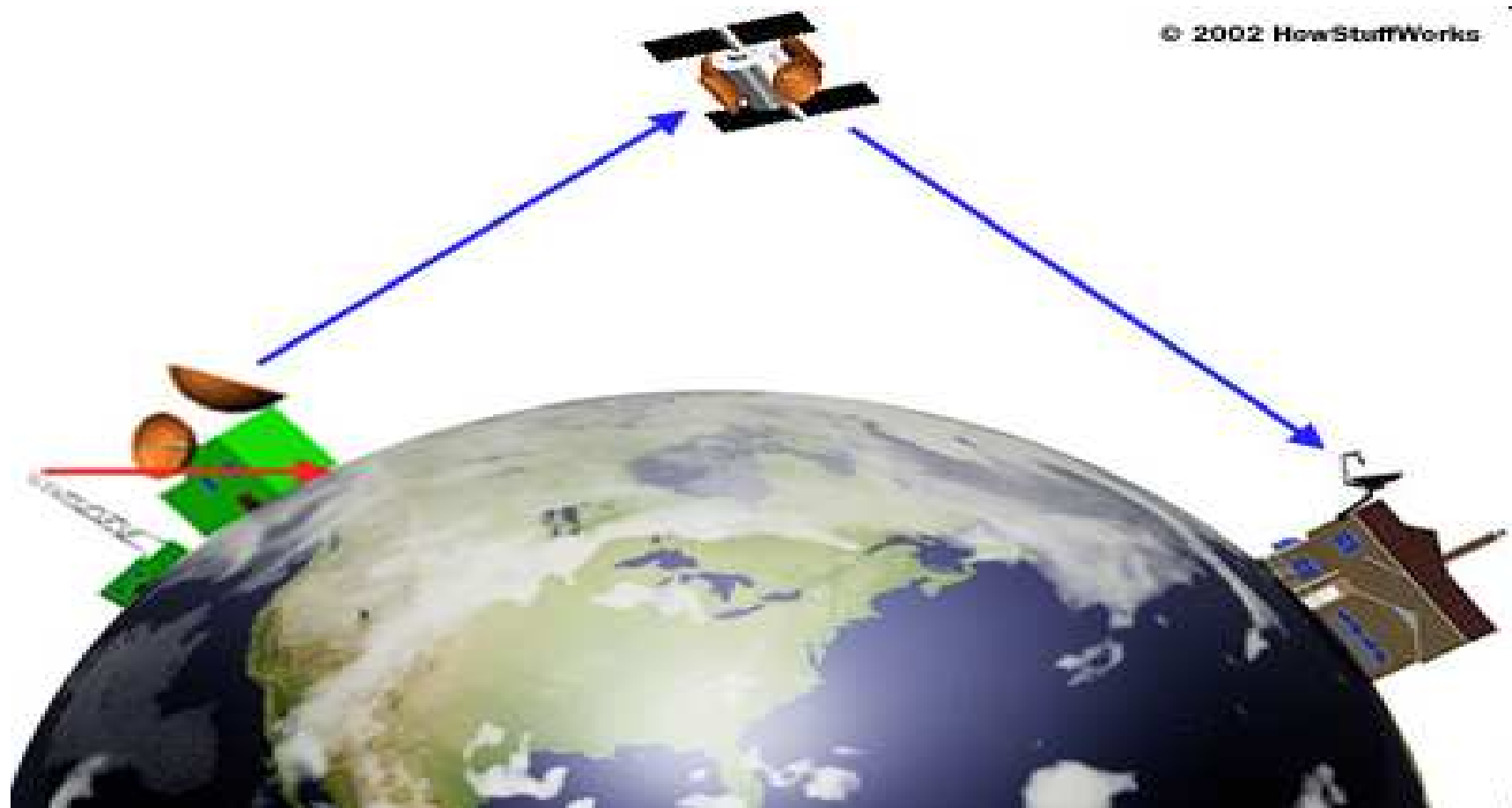
- No security, revenue loss if open systems/software.
 - Proprietary systems and decoders only need apply.
 - Hardware protections NECESSARY

Systems:

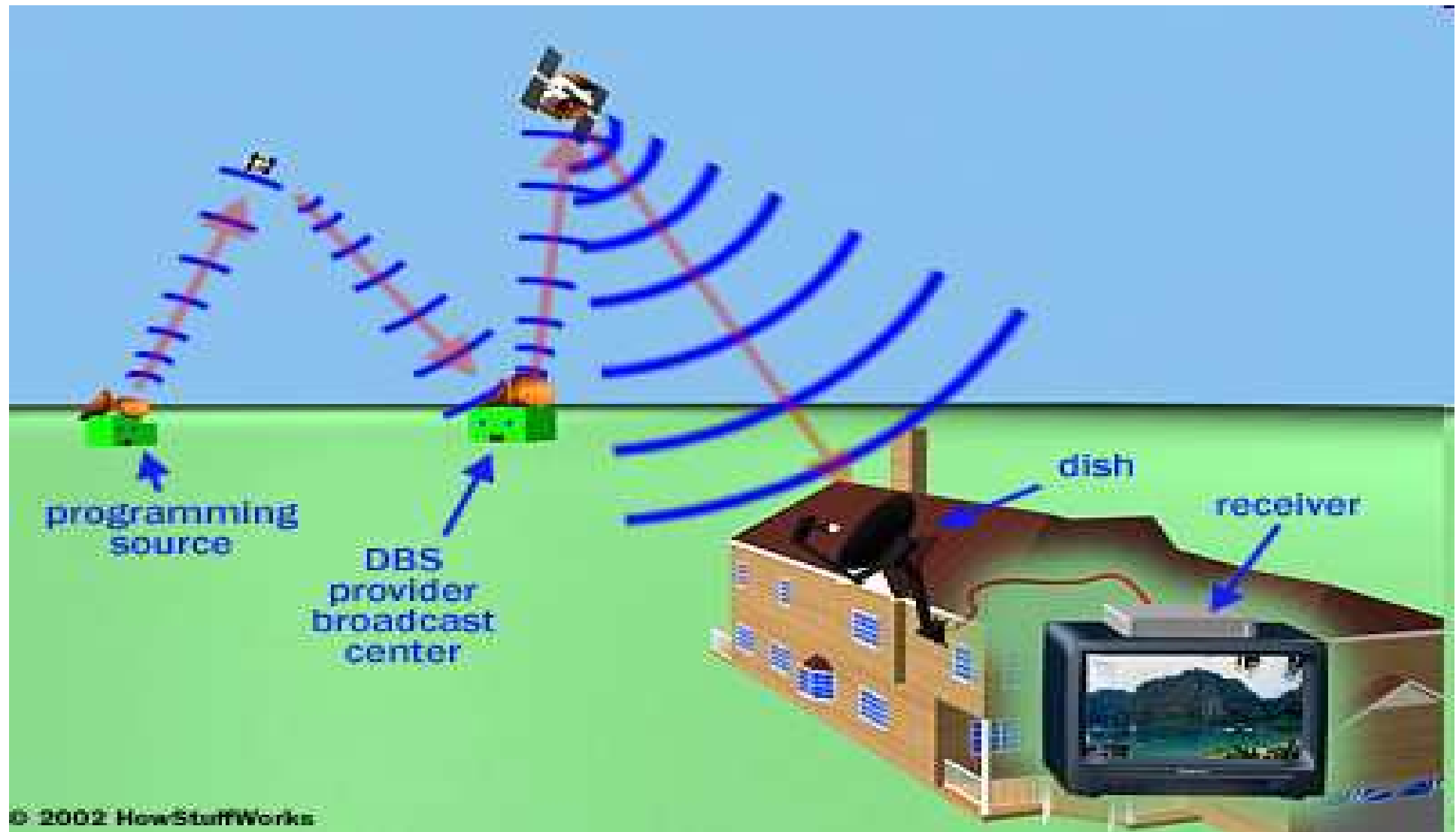
- Decoder / Set-top box: Standard
 - Descrambling/decrypting the image
- Smart cards: Security
 - hardware, tamper proof and reverse-engineering proof security, much better than USB tokens, less standard, much more maturity, e.g. hardware countermeasures)
 - Separate the security of different operators, Upgradable.
 - key management

Satellite TV

Almost Historical...



Still in Massive Use !!!!



Part 1:

Broadcast Encryption:

Past and Present (one-directional) Pay-TV

Hard Part

Part 2:

Bi-directional Pay TV:

Present and Future of Pay-TV

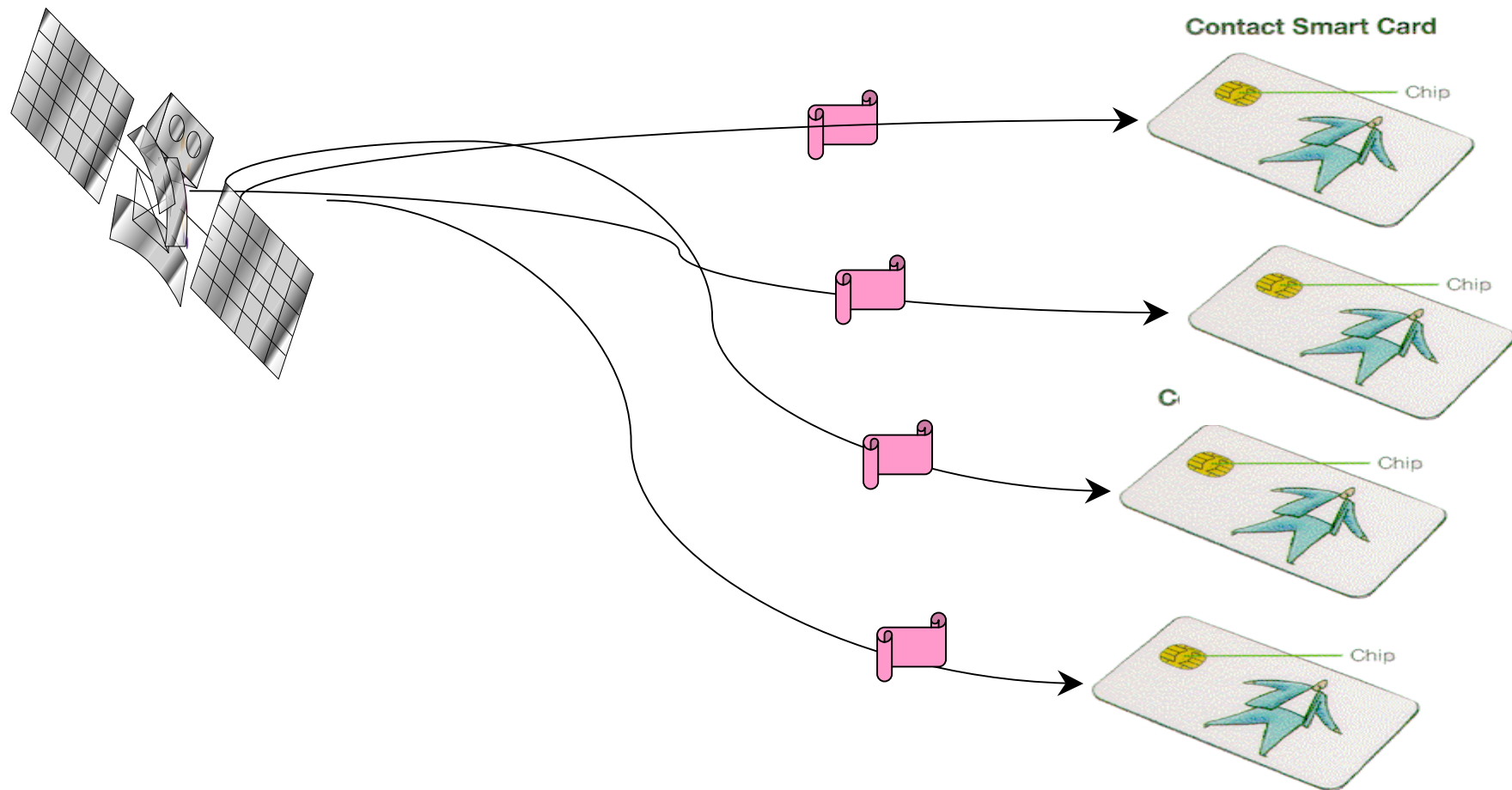
Easier Part

Part 1:

Broadcast Encryption:

Past and Present (one-directional) Pay-TV

One Direction



Evolution

1. Analogue systems
2. Hybrid systems
3. Digital transmission

Evolution of Broadcast Pay-TV

1. Analogue systems

- Scrambling
- No crypto / a little crypto
- Can be broken by signal processing techniques
- E.G. Early Canal+...
- still exist

2. Hybrid systems

- Better (?) scrambling
- Full cryptographic key management using smart cards
- Example: VideoCrypt, Canal +
- Still can be broken by signal processing techniques

Scrambling Methods

- No security:
 - Removing sync (LuxuCrypt, Holland RTL4 and 5),
 - Confusing automatic gain control (Macrovision VCR killer).
- Tiny Security:
 - Delay lines – early Canal +, delay 0, 902, 1804 ns.
 - Rotate certain lines – BSkyB, VideoCipher, VideoCrypt requires memory for a whole line.
 - The same with video inversion (OAK ORION).
 - Double cut in luminance and chrominance (EuroCrypt).
 - Permutation of lines (Canal+, Nagravision, ABC Canada).

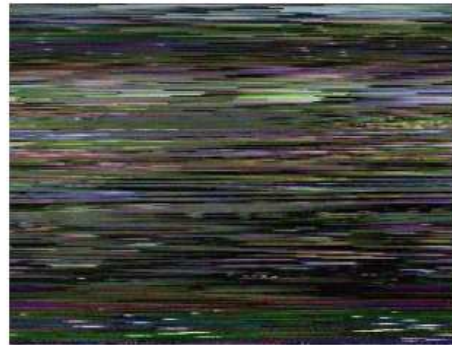
All can be broken by signal processing methods...
PC-TV cards + algo.

Example of Attack on VideoCrypt (M.Kuhn - Cambridge)

An Image Processing Attack on VideoCrypt



unscrambled source signal



broadcasted scrambled signal



result of cross-correlation with
cutpoints marked



edge detector avoids horizontal
penalty zones around cut points



final b/w descrambling result obtained
without knowledge of card secret

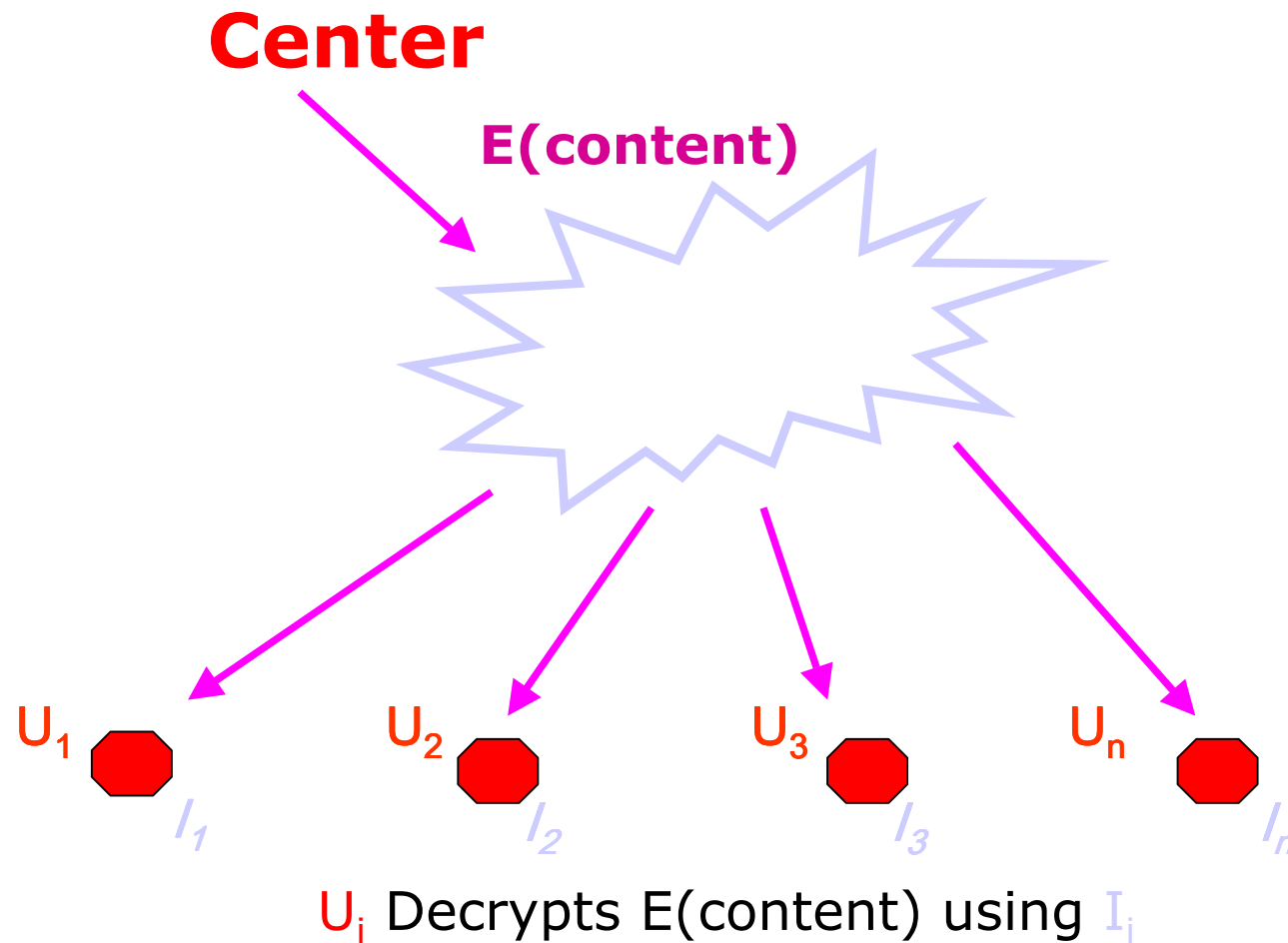
3. Digital TV

3. Digital transmission (MPEG-2 video and audio.)

- Can be really encrypted with cryptographic algos.
- Key/subscription management with smart cards
- Problem: how to distribute the transmission. Huge amount of data, in most cases image is encrypted with a CW (e.g. 64 bits),
 - The same for all users,
 - Valid for some 1-10 seconds.
 - Problem: how to distribute image CW.

Broadcast Encryption

Broadcast Channel == Broadcast Encryption



Broadcast Channel

Functionality:

- Sending the same signal to many people.
- Authorize some of them to receive a subset of it.
 - Dynamic update of the subset (subscribe/unsubscribe).

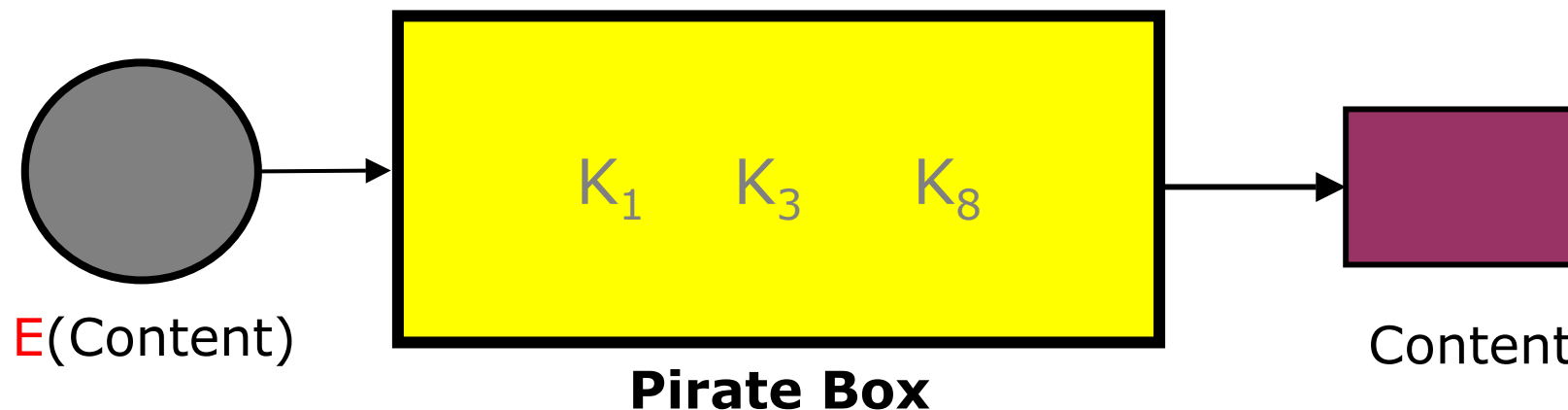
To Prevent:

- Various form of content/access sharing.

Broadcast Channel – The Danger

The problem:

- Various form of content/access sharing.
 - Example:
 - Users leak their keys to pirates
 - **Pirates** construct unauthorized decryption devices and sell them at a discount.



- Many other ways...

Approaches to Achieve Security

- Traitor Tracing [Chor Fiat Naor 1994]

- Trace and Revoke (combine both):

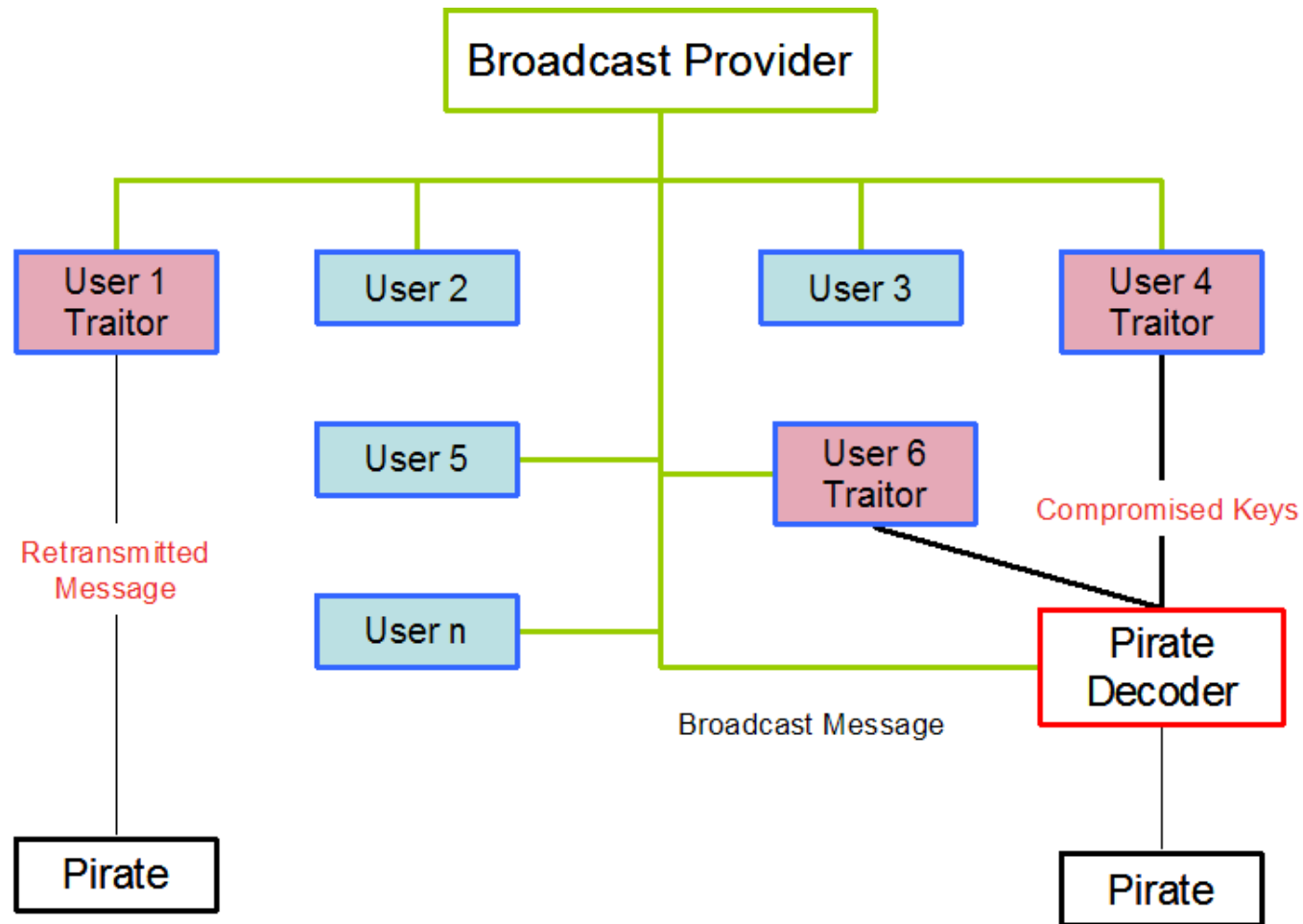
- **Trace** users who leak their keys
 - **Revoke** those keys - rendering pirated boxes *dysfunctional*.

- Self Enforcement [Moti Yung]

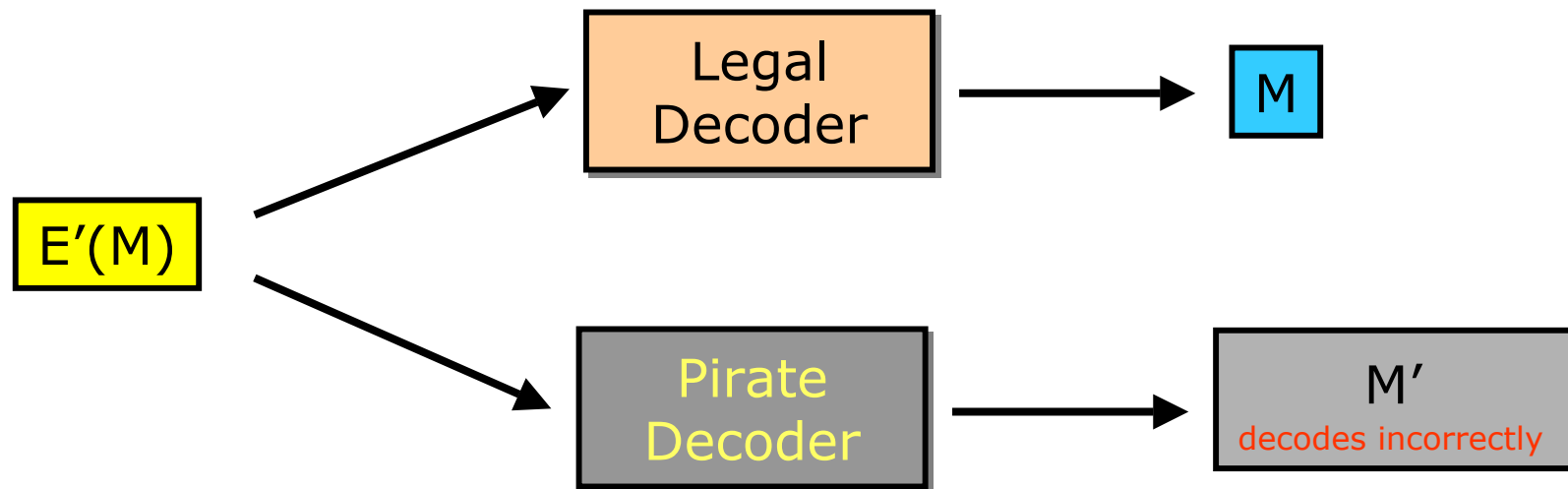
Goal: discourage users from leaking keys

- **Idea**: key should contain sensitive information that user doesn't want to spread. In addition: Should be impossible to use without revealing (e.g. black box revealing).
 - **Example**: name, credit card number, their salary...
 - PB: how to embed the sensitive information in the keys...
Related to ID-based crypto...

Traitor Tracing



Revocation



Broadcast Channel – Goals contd.

- **Traitor tracing:** Capacity to identify the origin of pirate decoders.
- **Black Box Traitor Tracing:** without opening the pirate decoder.
- **Resiliency** = C , usually small. Detect 1 out of C traitors.
 - Random resiliency: average number of users that can be detected.

Revocation is the most important goal.

Tracing: find the keys to revoke.

Dynamic Traitor Tracing: with revocation.

Broadcast Channel – Goals contd.

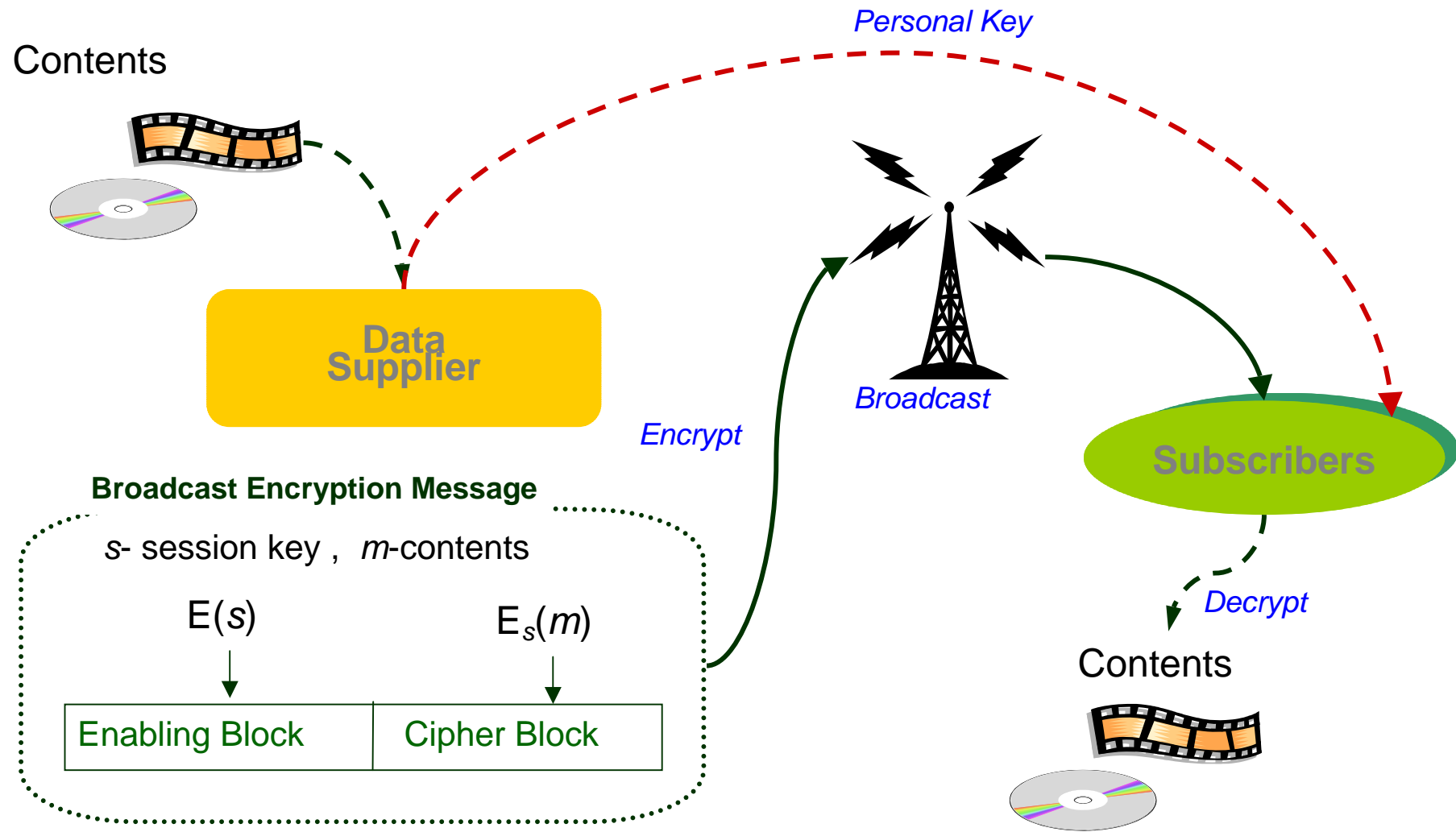
- Performance: many acute problems:
 - Low transmission
 - Low storage at user's end
 - Fast computation...

Theory to practice:

Partial formalisation of the problem, not obvious to apply in a sensible way, several pitfalls in applying it in practice.

1. Timing problems, (later)
2. All traitor tracing vs. performance issues (later)
3. The “absent user issue” – comes as a limitation at several points.

Broadcast Encryption - Practice



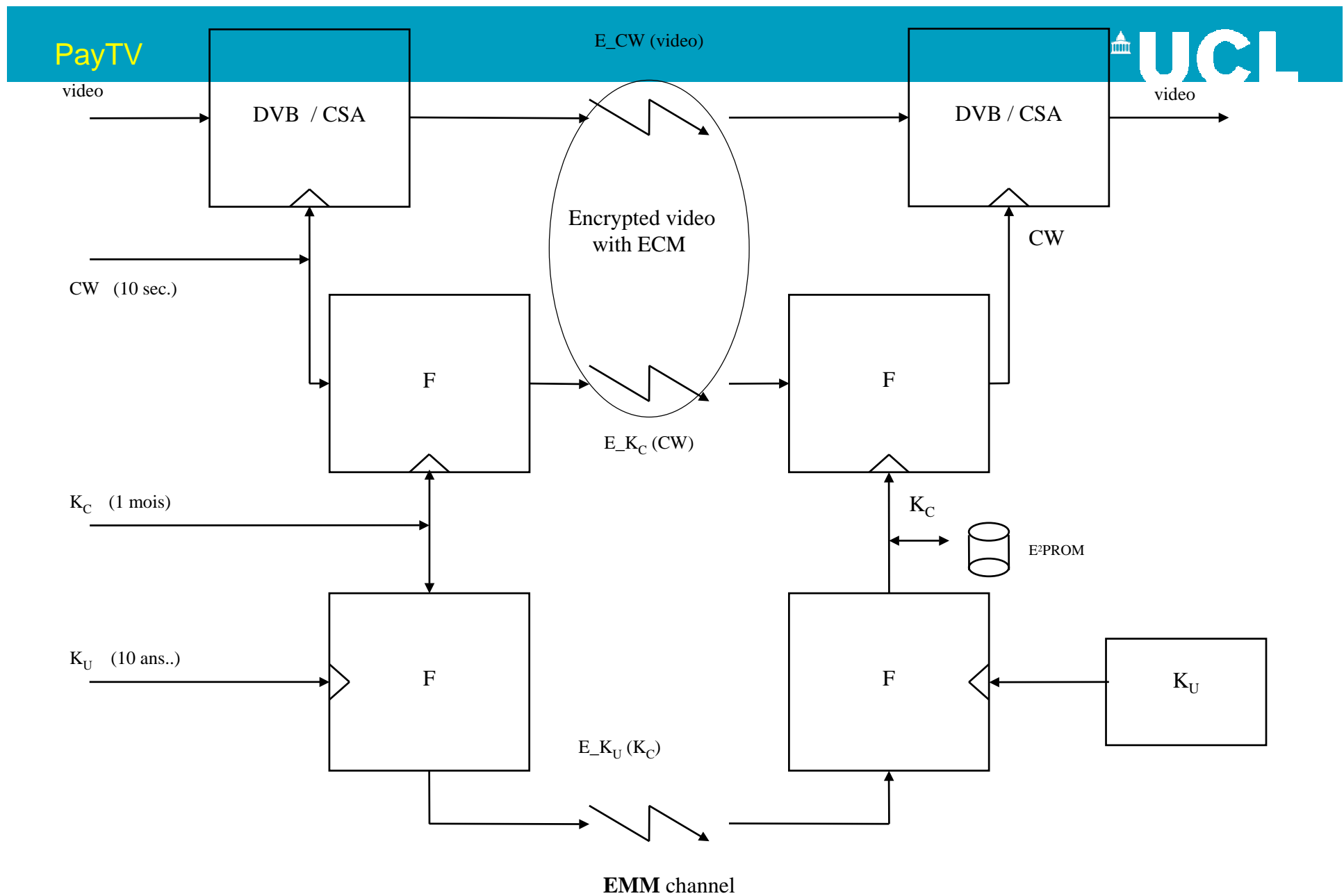
DVB – type systems (e.g. Viaccess)

Standard, popular, mainly in Europe.

- A decoder = set-top box
 - A smart card
 - Standard (but secret and hardware) common scrambling algo
 - Proprietary access control systems on a smart card.
 - System allows SimulCrypt:
- Several access systems for the same emission (e.g. on a satellite). Decrypt the same control words by different methods.

Data Flow - 3 levels

- CW: control word
(mots de contrôle)
- ECM: Entitlement Control Messages sent with the content,
 - distribute CW
 - not individual
 - few bytes(Messages d'Exploitation)
- EMM: Entitlement Management Message:
 - Individual for each card
 - sent much in advance (e.g. 1 month), better bandwidth
 - rights management, parental and geographic control
 - Security management, update, etc..(Messages de Gestion)



What Cannot Be Avoided (1)

- Video sharing:

Diffusion of the descrambled content:

- Real time (web-server – not done, VHF 100 m – available)
- Delayed: VCR, DVD, DivX.

- Bad news

- In most cases nothing can prevent it.
 - Capture TV signal
 - Capture digital MPEG-2 stream – inside the decoder.
- Solution: descramble inside the TV, not used so far [Thomson].
- Partial solution: DRM video card with analog output (still can be digitalised, not really interesting).

What Cannot Be Avoided (2)

- Real-time card sharing:

CW: plaintext between decoder and the card.

Diffuse CW instead of Video + modified decoder coupled with a PC: *McCormac Hack [still works in Spain...]*.

- VideoCrypt: 60 bits every 2.5 seconds.
- Usual DVB systems: 64 bits every 10 seconds.
- Old proposal, not used a lot.
- Again nothing can prevent it.
 - Deterrent: the source can be identified.
 - Threat: anonymous file distr. systems on the internet.
- MUCH WORSE: in the current system:
if F known, monthly K_C is enough (the same for everyone).

What Can Be Avoided But Is Not

- Worse Real-time card sharing:

Monthly K_C (sometimes even lasts longer) is diffused.

Can produce false cards. The attack works when the algorithm F is public, see later.

CAN BE AVOIDED – Courtois-Patarin patent – see later.

What Cannot Be Avoided (3)

- **Offline Card Sharing** – Gets Worse. (a.k.a. VCR attack ?).

Common Practice Among Hackers.

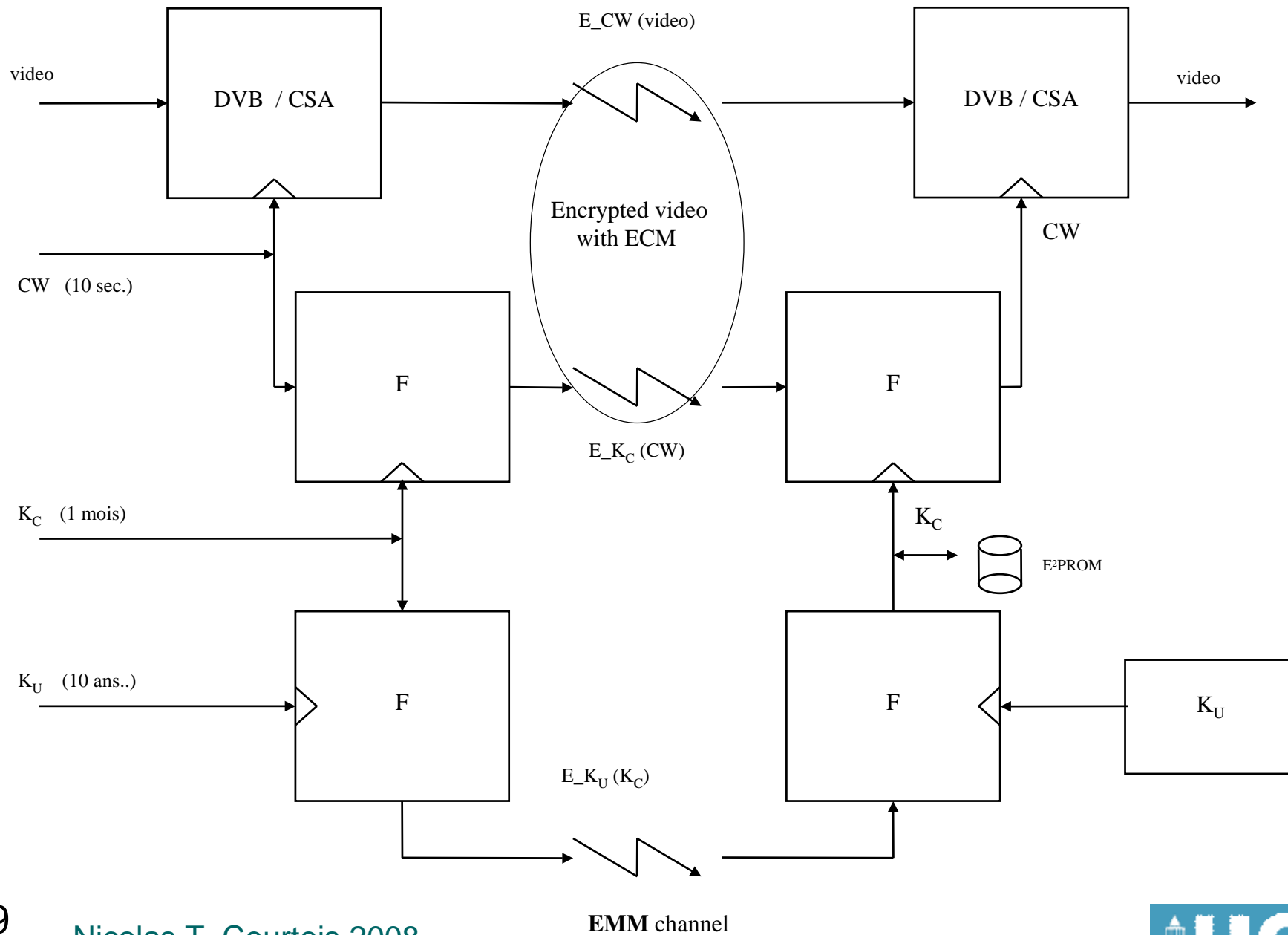
- Diffusion of CW can be delayed.
Store them in a logfile (VideoCrypt –VCL files).
- Record the scrambled signal.
 - Old VideoCrypt: the whole signal could be recorded and replayed with a normal VCR.
 - Current MPEG-2 systems: use modified decoder / PC satellite receiver. Capture the digital encrypted stream and record on a hard disk.
- Replay the scrambled signal next day with the stream of CW.

What Cannot Be Avoided (4)

- No return channel: (pas de canal ascendant).
Consequences:
 - Clones of one legitimate decoder will work for some time.
 - Cannot detect before sold to many people.
 - Must follow pirate market.

What Can Be Avoided

- Realistic **goals**:
 - minimize loss of revenue. Discourage pirates. Keep the number of pirate decoders small.
 - update the system frequently and improve it
 - problems of one operator should not affect the other
 - prevent very large scale / industrial piracy – InterPol, prosecution is necessary... Discourage people from buying pirate decoders.
- **MEANS**:
 - Buy pirate decoders, disassemble them, study them,
Company MUST follow the hacker activity.
 - Deactivate/Revoke the compromised systems if you can – complex problem, see later. Cost/Performance problems.
 - Trace (coalitions of) traitors – also a complex problem ...



Timing and Bandwidth Issues

Very Important!

Timing Issues (level 1)

- Life (CW) = 10 seconds.
 - Can be 2-10 sec.
- Cannot be much shorter – time to receive ECM. Limited memory in the card to store CW. Limited bandwidth of ECM channel.
- Cannot be much longer:
 - real-time card sharing will become easy. Cryptographic attacks could become possible – break CSA (proprietary algo, now published on the internet - FreeDec end 2002, could be broken soon).
 - The user that just switched his decoder cannot wait more than 10 seconds.

Timing Issues (level 2)

- Life (K_C) = 1 month.
- Cannot be much shorter – time to receive EMM.
 - Limited memory in the card to store several of them in advance.
 - More important: Limited bandwidth of EMM channel – for each card individually, millions of cards !!!!
- Cannot be much longer:
 - If the algo F is compromised (usually is – reverse engineering the smart cards, happened many times) then K_C allows to distribute pirate cards valid for the current month.
 - If the user switched his decoder on after 1 month of absence, will have to wait minutes/hours, will call the distributor etc. Limit the cost of this.
 - Some current systems: the key is never changed, pirate cards exist.

Timing Issues (level 3)

- Life (K_U) = few years.
- Cannot be much shorter – cost of issuing new cards.
- Cannot be much longer
 - the whole system has to be updated anyway due to other attacks.
 - every tracing traitor system has a limited capacity. if many users give away their keys there is no revocation possible.

Timing and Bandwidth

Courtois-Patarin Solution [patented]

Timing Issues – Our Patent

Patented by Nicolas Courtois and Jacques Patarin, as a byproduct of the Viaccess 3.0. Study. [2001]

Pirates have:

10 s instead of 1 month.

- **Even if F is compromised.**
- **Traitor Tracing Capable Otherwise.**

Timing Issues – Our Patent

Problem:

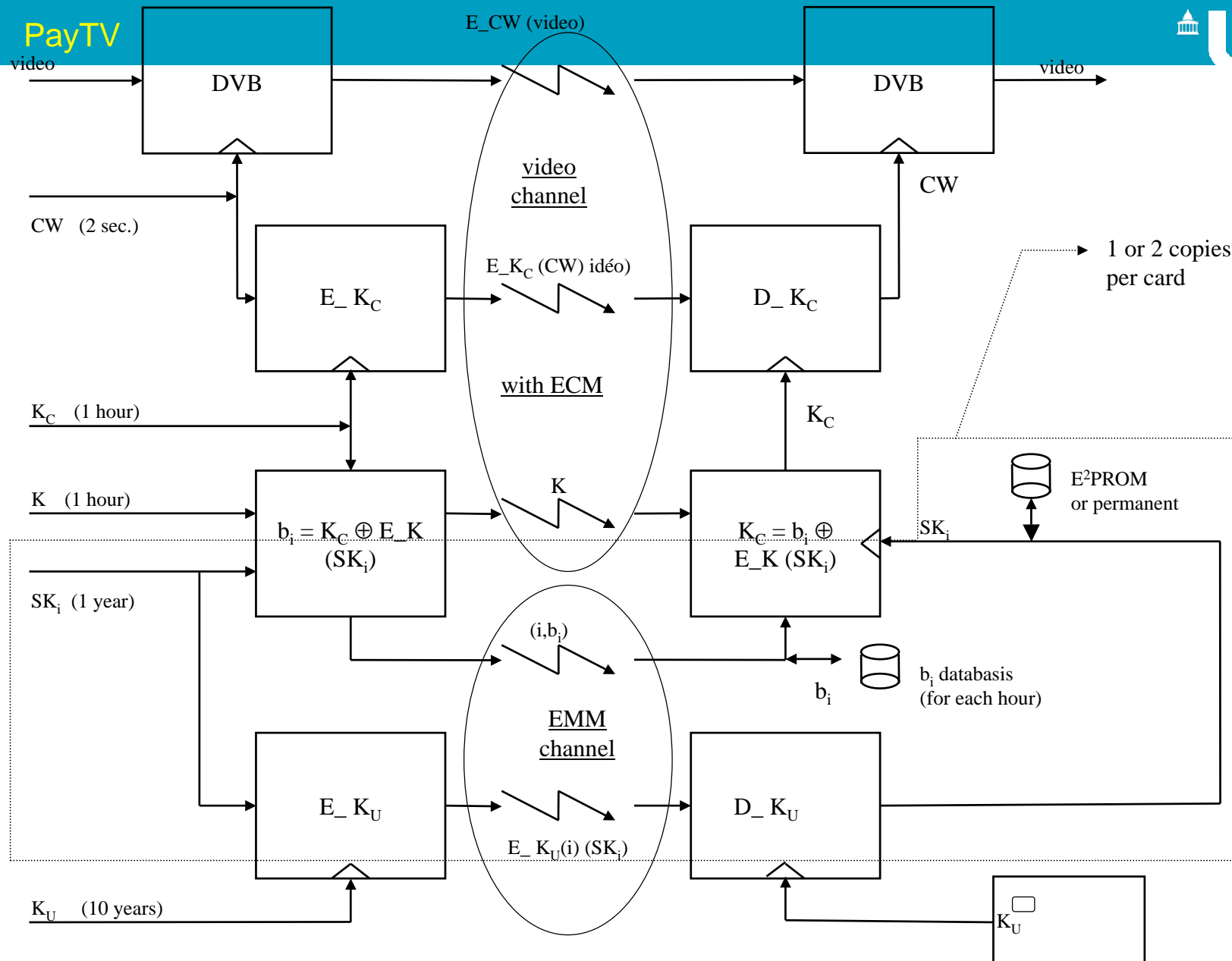
- At present K_C is sent to the cards in advance by ECM.
- When the pirates reverse-engineer one card, they find the algorithm F , and the key K_C .
- Potentially millions of pirate cards for 1 month (or more) not traceable at all ! (Have been done).
- Our patent: secret key technique, allow to render K_C traceable, yet to sent it in advance to everyone by public low-bandwidth channel.

Courtois-Patarin Patent – Traceability

- K_C is sent in advance to everyone by a private channel.
- One piece is missing. This one is
 - Necessary
 - sent in the last 10 s.
 - TRICK: it is the same for everyone !!! Main point in the patent.

Called **PRO-ACTIVE SYSTEM**. Combines:

- The bandwidth capacity as if was sent at the last moment,
- The tracing capacity of things send beforehand addressed individually to each card.
- Transparent: Can be combined with any combinatorial secret-key traitor tracing scheme.



Combinatorial Security

Systems Resilient to Piracy

Tracing and Revocation

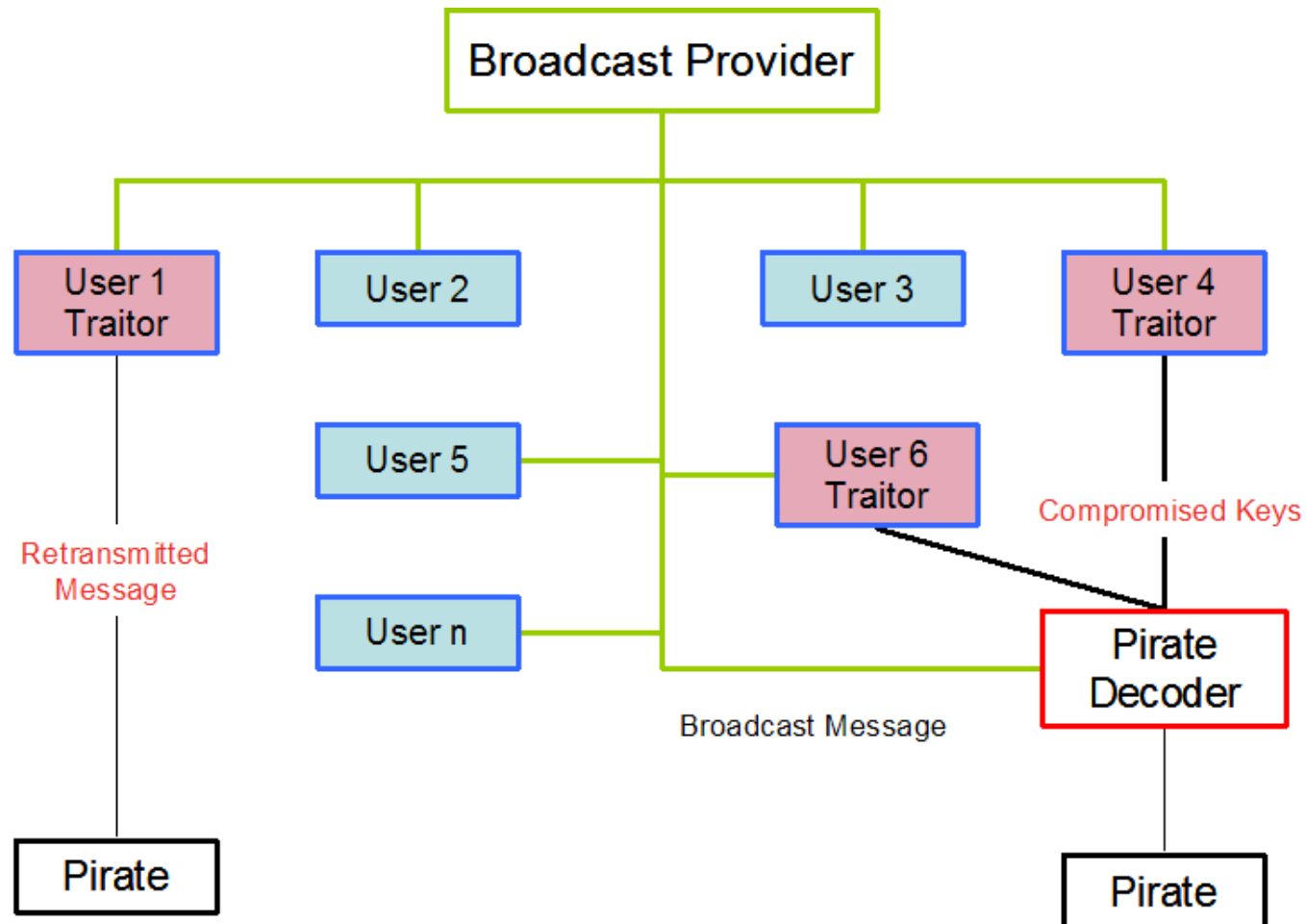
Resilience

Tolerate a certain degree of Piracy. React, Adapt in Real Time.

Options:

- Up to a certain level:
 - Accept, may be good for sales [decoder/smart card vs. owner of the content]
 - Pay TV broadcaster: no evidence if this has to be bad for sales...
- Detect pirate activity/market [organised fraud/criminality] and analyse them. =>
 - Disable pirate decoders and keys they contain
 - cf. BlueRay system
 - Easy and feasible
 - Beware coalitions of pirates!
 - Not so easy anymore...
 - Update cards (2 years), their memory (may take ages too).
 - Update crypto algorithms too...

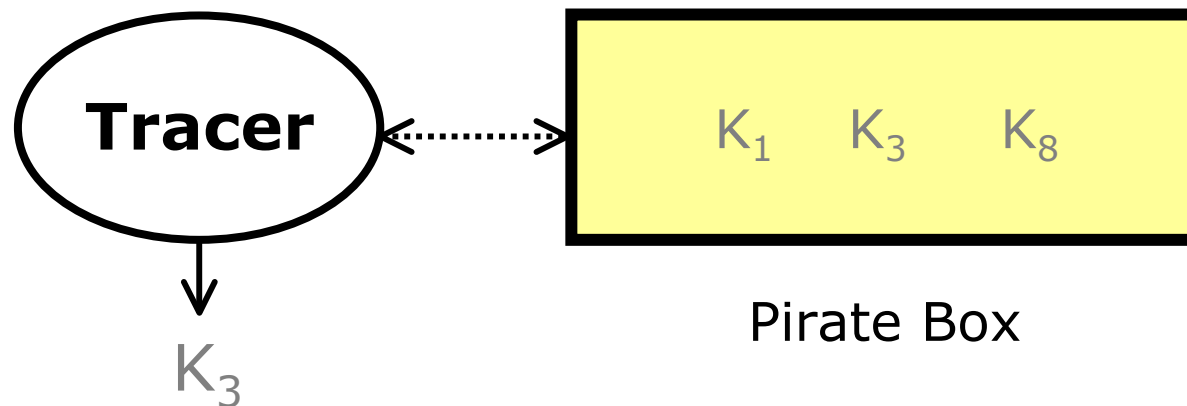
Traitor Tracing



Main Goal of Traitor Tracing

Goal of Traitor Tracing Schemes:

- Find source of keys of *illegal* decryption devices
- If at most t traitors - should identify (one of) them
- No honest user should be implicated (Pb.)



Goals of Traitor Tracing

- Fighting Piracy

- Identify piracy
- Prevent transmitting information to pirate users
- Identify the source of piracy

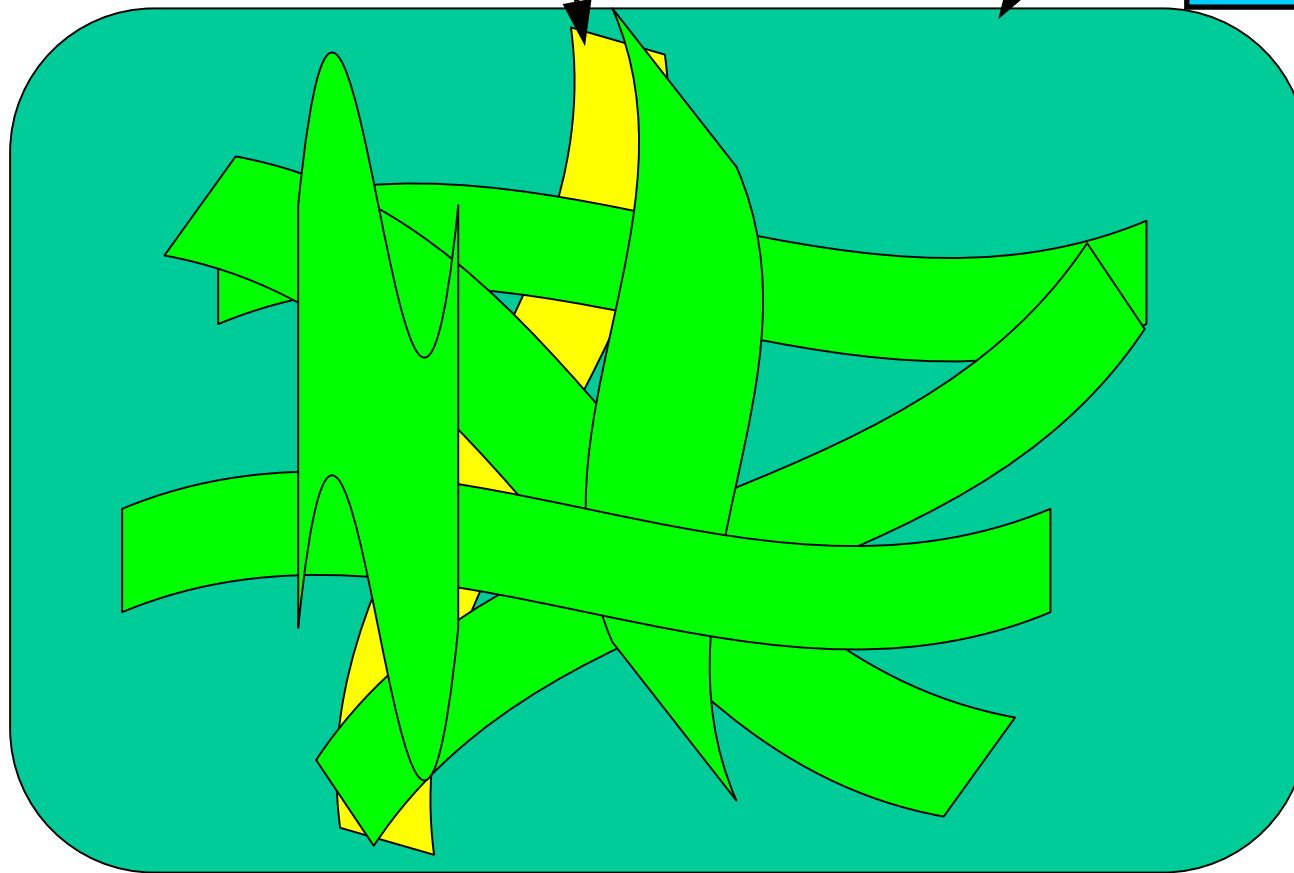
- Consideration

- Memory and Computation requirements
 - Per authorized user
 - For the data supplier
- Data redundancy overhead

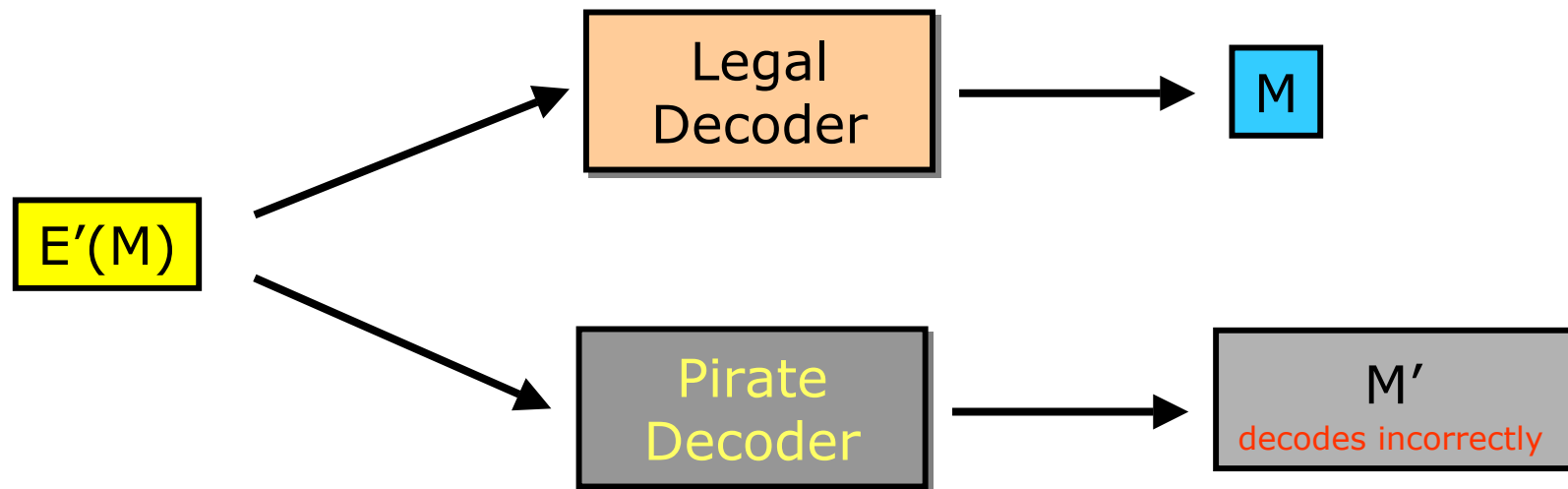
The Guiding Principle

The keys of one receiver R

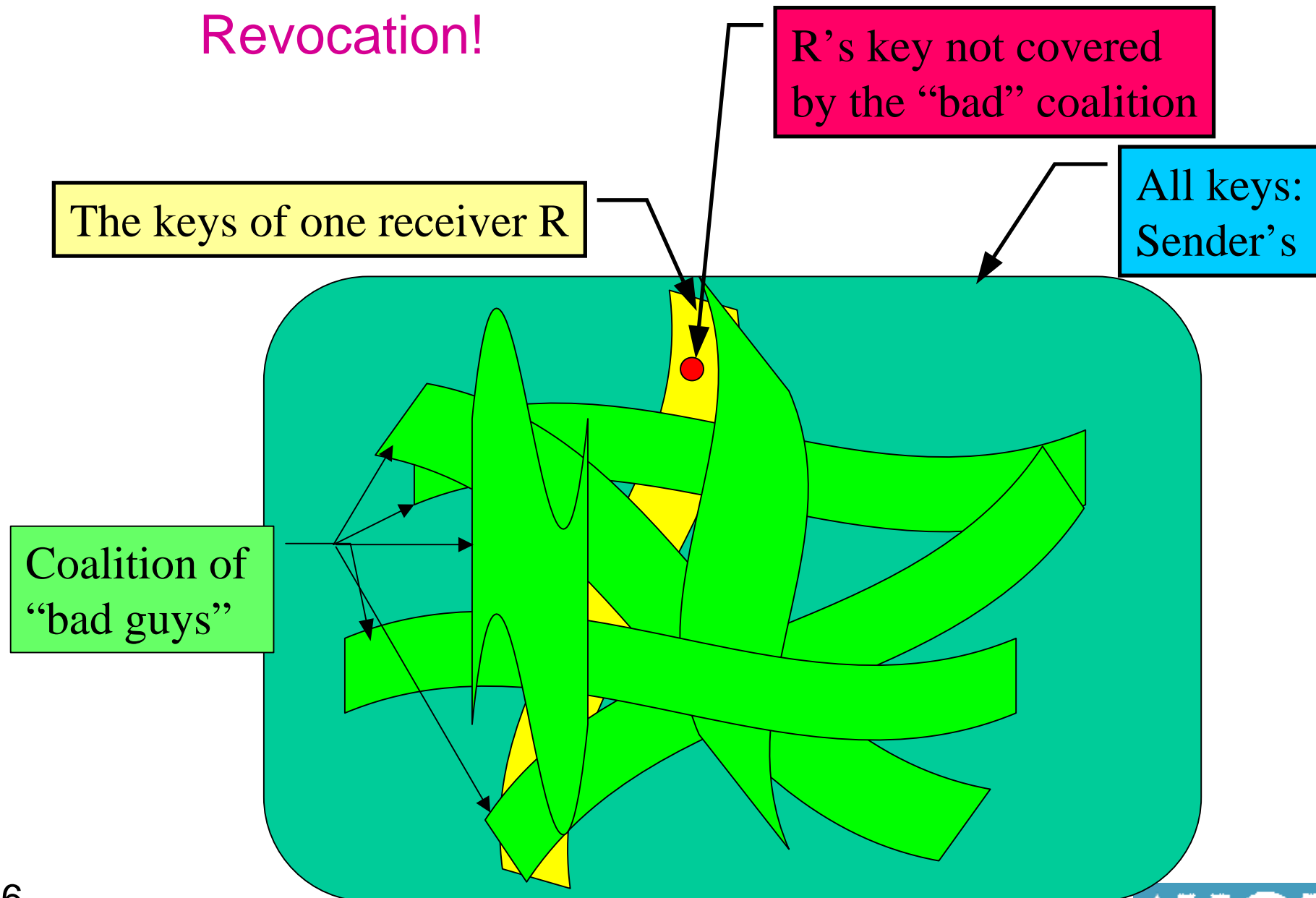
All keys:
Sender's



Revocation?



Revocation!



Tracing And Revocation

Traitor Tracing

Every user uses “different keys” to access the same content.

At what level we trace ????

- For CW : impossible, few bytes only are available.
- For K_C : possible but requires maybe to decrease the duration of K_C – otherwise it can be diffused on the internet. (again if F is also compromised). (Life of K_C : Can be 1 day or 1 hour)
- Plan:
 - 1) We describe the solutions for K_C and then:
 - 2) MIRACLE: these can be applied “in a way” on a CW level:when combined with Courtois-Patarin patent.

Traitor Tracing

Every user uses different keys to access the same content.

- Classical constructions:
[Chor, Fiat, Naor, Pinkas 1994-98]
- Public key versions: Boneh-Franklin [1999],
Barbain-Gilbert [2003].
- Classical Traitor Tracing: [Chor, Fiat, Naor, Pinkas 1994]
–combinatorial solutions, not trivial, many parameters.
 - Use redundancy to send the data.
 - Disable some “channels” that have been compromised.

A Simple System that Works

Traitor Tracing

Every user uses **different keys** to access **the same content**.

STEP 1: SHARE THE KEY.

k out of n are necessary to access the content.

Techniques based on MDS codes or Reed-Solomon codes.

Simple case: $k=n$.

Simple Traitor Tracing

Every user uses **different keys** to access **the same content**.

Simple method.

$$K_C = K_1 \oplus K_2 \oplus K_3 \oplus K_4$$

Each of them is necessary to decrypt.

Each of them is sent by “a different channel”.

Traitor Tracing

$$K_C = K_1 \oplus K_2 \oplus K_3 \oplus \dots \oplus K_n$$

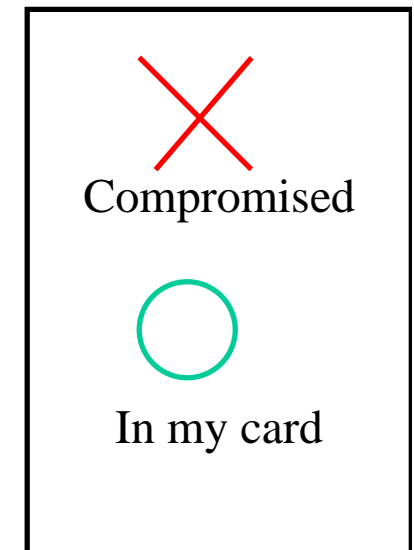
To decrypt K_1 use K_{11} or ~~K_{12}~~ or ~~K_{13}~~ or K_{14} ... K_{1m}

To decrypt K_2 use K_{21} or K_{22} or K_{23} or K_{24} ... ~~K_{2m}~~

To decrypt K_3 use K_{31} or ~~K_{32}~~ or K_{33} or K_{34} ... K_{3m}

.

To decrypt K_n use K_{n1} or K_{n2} or ~~K_{n3}~~ or K_{n4} ... K_{4m}



Simple Method

$$K_C = K_1 \oplus K_2 \oplus K_3 \oplus \dots \oplus K_n$$

Transmission:

- $n \cdot m$ messages each time
- n keys per card sent in advance

If C cards have been compromised, use only $m - C$ keys per row.

- Most of the cards will not work.
- This method is not very good.

Good tracing - poor revocation.

Another Version

Use 1 out of n secret sharing.

If C cards have been compromised, use only $(m-C)$ keys per row.

- Cards that will not work = small, about $(1 - C / m)^n$
- Better real-time revocation.
- Still not very good: in practice there are also cards that are already compromised but we do not know it yet. Also the tracing identifies one of the keys. We will find only some of the pirate keys.

New Trade-off: if we mix known and unknown pirate keys, use 2 out of n or 3 out of n in order to tolerate some unknown pirate keys.

If a pirate card uses only unknown pirate keys, smaller coalition, easier tracing.

More Advanced [Research] Proposals

Goals

- **Given**
 - **N** (# of receivers)
 - **b** (# of “bad guys”)
- **Find smallest k (# of keys) and N subsets $S_i \subseteq [1, \dots, k]$, such that for**
 - deterministic:
 - any **b+1** subsets $S_{i_0} \not\subseteq S_{i_1} \cup \dots \cup S_{i_k}$
 - probabilistic:
 - $\text{Prob}[S_{i_0} \subseteq S_{i_1} \cup \dots \cup S_{i_k}] < p$

Problems with Classical Traitor Tracing [Chor, Fiat, Naor, Pinkas 1994-98]

- Large message size. Best results $O(C)$, $C=nb$ of traitors.
Worse if the key size has to be small too !
 - Probabilistic identification of traitor. Will not hold in court.
Deliberate framing of innocent people.
 - In practice
 - Tracing is not so important: A deterrent. Penal perspective.
 - Revocation is important (disable known pirate decoders).
 - Black box property is important.
- Not easy: the decoder can avoid being traced, giving false answers, or be recognizing the tracing algorithm. **Not solved completely.**
Not solvable for a tamper-proof pirate decoder.

Combinatorial Schemes [Chor, Fiat, Naor, Pinkas 1994-98]

	PROPERTY	SECTION	Personal KEY	Data Redundancy	Decryption Operations
Secret 2-level	Best fully-resilient	3	496	21270000	496
Threshold	One-level, min. Data redundancy	4.1	53000	4000	1
Threshold	Two-level, min. Data redundancy	4.2 $W=1/2$	1660	185000	9
Threshold	Two-level Min. key	4.2 $A \rightarrow \infty$	380	1290000	13
Threshold	tradeoff	4.2 $W=1/8$	10000	54500	3

Complexity of different Tracing Traitor schemes
Using $n=10^6$, $k=1000$, $q=3/4$

Example 1

[Chor, Fiat, Naor, Pinkas 1994-98]

One proposed example:

- 1 million users
- 500 cards are compromised by pirates (per month)
 - 6300 keys / card.
 - 27 500 blocks sent each time
- Can black-box-trace one of the traitors with probability $999/1000$ if the pirate decoders work with probability $\geq 3/4$.

Example 2

[Chor, Fiat, Naor, Pinkas 1994-98]

Second proposed example:

- 1 million users
- 500 cards are compromised by pirates (per month)
 - 26 500 keys / card.
 - 2000 blocks sent each time
 - Can black-box-trace one of the traitors with probability 999/1000 if the pirate decoders work with probability $\geq \frac{3}{4}$.

Main Limitation of Classical Traitor Tracing

[Chor, Fiat, Naor, Pinkas 1994-98]

- Tradeoff: Large message expansion – large key size.
- Neither is possible in smart cards + ECM channel.
- Their application is therefore limited and cannot resist large coalitions of traitors (>500 or so).

Better Methods – Not so Bad...

ALL SUCH COMBINATORIAL TRAITOR TRACING SCHEMES

Have the same problem:

Unable to resist to large coalitions of traitors with reasonable transmission + storage requirements – theoretical limits.

LESS SERIOUS THAN THOUGHT !!!

Update all the system monthly by addressing individual cards (by K_U).

How to do Efficient Traitor Tracing - Practice

- Update the whole system monthly.
- Adjust the combinatorial scheme to the context.
Several parameters. Several schemes. Not easy at all.
- Choose a version with reasonable storage requirements
(e.g. 6300 keys/card)
 - Then we have e.g. 27000 values to transmit.
 - Combine with Courtois-Patarin patent.
Dramatically reduces the size transmitted at the last moment, most information transmitted 1 month in advance.
- All cards/pirate data emitted less than 10 seconds before
Can be traced.

Better Recent Schemes

	CFNP Open 1-level	Boneh Franklin	Lee, Kim Lim	Tzeng Tzeng
Private Key	$O(k^2 \log m) * H $	$ q $	$2 n + \Phi(n) + q'$	$ q $
Length of Encryption Block	$O(k^4 \log m) * H $	$(2k+1) * p $	$3 n + \Phi(n) + \{O(z) + p' \}$	$O(z) * p $
Compute amount of Encryption	$O(k^4 \log m)$ XORs	$\approx (2k+1)$ Exps. (mod p)	1 Exp. + 2 Mls. (mod n) + $\{O(z)$ Exps. (mod $p\}$	$O(z)$ Exps. (mod p)
Compute amount of Encryption	$O(k^4 \log m)$ XORs	$\approx (2k+1)$ Exps. + $(2k+1)$ Mls. (mod p)	2 Exps. + 2 Mls. (mod n) + $\{O(z)$ Exps. + $O(z)$ Mls. (mod $p\}$	$O(z)$ Exps. + $O(z)$ Mls (mod p)
# of Revocation	—	—	∞	$\leq z$

m : # of users, k : revocation capability, H : hash ftn., p, q : prime number, $|p| > 1024$, $|q| > 160$, $q|(p-1)$, z : Shamir degree of polynomial, modulus of n -RSA $|n| > 1024$, p', q' : prime, $|p'| > |n|$, $q'|(p'-1)$

Boneh-Franklin Traitor Tracing

[Boneh-Franklin 1999]

Evolution of an earlier scheme by Kurosawa and Desmedt:

broken, the authors showed that the keys can be traced, but did not think about combining keys in a trivial way to form new keys that cannot be traced.

Typical pitfall in crypto ! Show the necessity of formal definitions of security in crypto !

Boneh-Franklin Traitor Tracing

- A **public key traitor tracing** scheme.

The emitter uses only public quantities: cannot produce false decoders, cannot frame innocent users to cover the leakage.

- Tracing is **deterministic**, no doubt in court.
- Better performance: eliminate factor $\log_2(\text{number of users})$. Important improvement in practice, $\log_2(1000000) = 20$.
- **Keys are short** (e.g. 160 bits), not $O(C)$ $C = \text{nb of traitors}$.
 - Size of messages: $2C+1$.
 - Computation: $2C+1$ exponentiations.
- Can be based on arithmetic or elliptic curves. Can be compatible with some PKI. Provably secure w.r.t DL problem. Top class scheme.
- Drawback: still problems with efficient BB tracing. No perfect solution?

Another Public-Key Solution

- Proposed by Henri Gilbert (France Telecom) in 2003/2004. Published at AsiaCrypt 2003. Patented for France Télécom.
 - Covered by ongoing X-CRYPT RNRT project.
(evaluation, improvement etc...)
 - Based on Sflash [Courtois, Patarin, Goubin] and multivariate polynomial schemes of Patarin.
 - A new type of block cipher
 - Several versions of the same block cipher can be constructed
 - They are used to decrypt CW or K_C .
 - The hacker can copy a cipher (allows traitor tracing) but cannot mix/modify them.
 - Best attacks: IP problem.
[Nicolas Courtois, Louis Goubin, Jacques Patarin, EuroCrypt 1998].

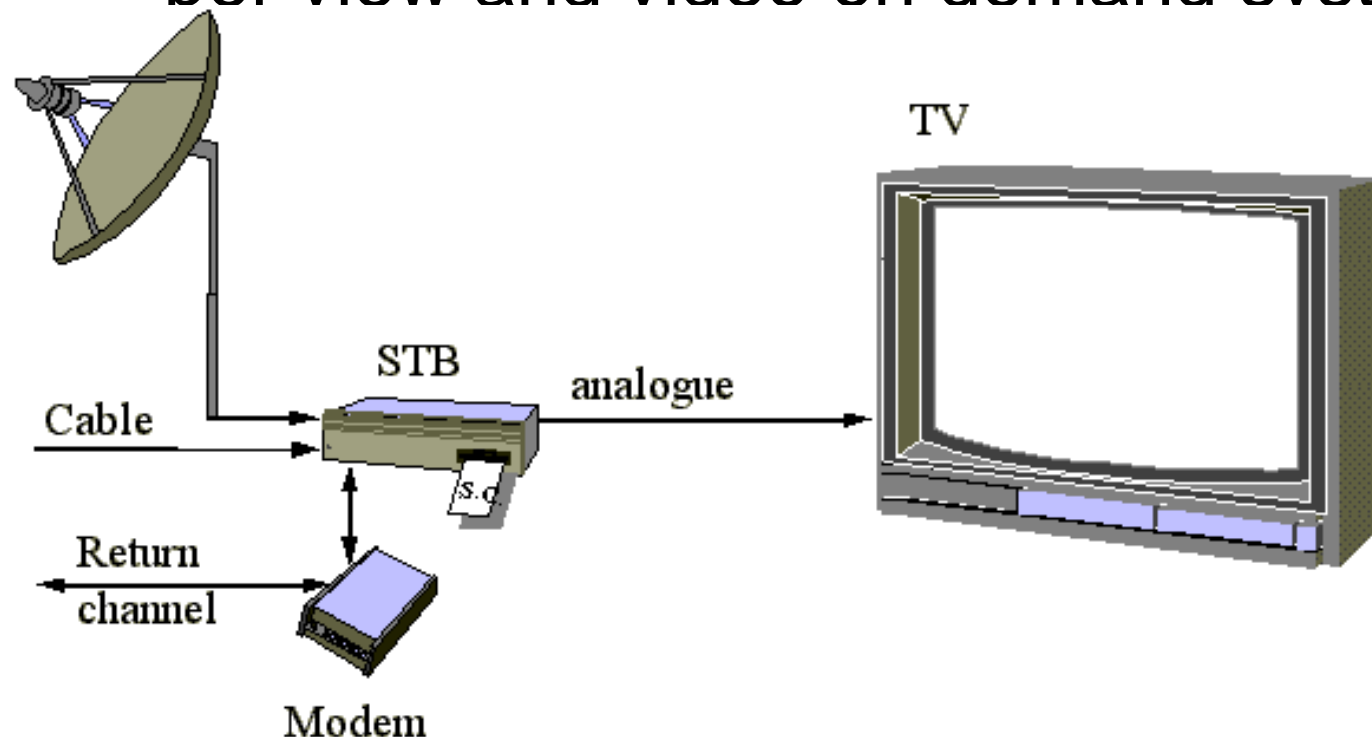
Part 2:

Bi-directional Pay TV:

Present and Future of Pay-TV

Modern Pay-TV

Bi-directional. (existed before, especially in pay per view and video on demand systems e.g.



Modern Pay-TV – Bi-directionnal

E.g.
BT Vision, 9Box, Freebox etc..

In theory the same that
any type of electronic commerce with immaterial goods.

In practice very different:

- Revenue loss and no security if open systems or software.

Owners of the content will not allow it:

- Proprietary systems and decoders only need apply.
- Hardware protections NECESSARY - smart cards are welcome !

Modern Pay-TV – How to Do It

Much easier, new possibilities.

- Use any payment system (bank card, subscription etc..)
- Can send individual content to any user, no limits to bandwidth in traitor tracing.
Or send the same content (cable) with CW that changes every 0.5 second and is transmitted in real time via internet.
- Allows watermarking [only as addition, weak security !].
- Much stronger properties are possible:
Non-repudiation is possible: the user signs digitally that he received the content. Makes prosecution of individual traitors really possible. (So far – prosecute those who produce / sell / use pirate devices).
- SOLUTION: We can allow to **maintain permanent private channels**. All the security problems are solvable by standard cryptographic techniques with, for example smart-card public key solutions.

Lessons Learned

- Pay-TV providers MUST follow the hacker activity in real time.
- Smart cards are unsuitable for holding global secrets. Secret algos can be compromised within weeks/months.
- **Local secrets**: public key techniques maximize the security.
- Uni-directional case: solutions exist. Not perfect. Courtois-Patarin patent improves and can be combined with virtually all of them.
- In bi-directional case, all the security problems are solvable by standard means , SK techniques, and better with PKI.
- PKI is a key argument to sell **smart cards**.
- **Public key protections** in general: Key element to solve about all security problems. At good level of security: need PK techniques, necessary to securely store/generate/use keys.
Future: it will be the main and the only reason to use smart cards ?