Cryptography Made to Measure

Workshop on Applied Cryptography
NTU, Singapore
December 3, 2020

Matt Robshaw
Orange Labs
Paris, France

A New Kind of Network …

- Telecommunication companies like France Télécom / Orange are used to managing networks; typically on a global scale

- However we now see the emergence of new types of networks

  - Sensor networks … capillary networks … personal area networks … supply chain logistics … m2m … Internet of Things … RFID tags …

- The pervasive nature of future deployments will have profound societal impacts …

RFID Tags – The Issue(s)

- We expect RFID tags to be deployed widely … and an RFID tag identifies itself to anyone who asks
  - But do we (personally) want this ?
  - What safeguards do we need to satisfy confidentiality and/or privacy goals ?
- On the positive side, can we leverage the fact that RFID tags will soon be attached to every item ?
  - Would it cost much more to also authenticate the tag (and product) ?

UHF Tags

- These are small, cheap, communicating devices
  - No internal power source
  - Operational range of 4-8 m
  - Multi-tag environments
  - Multi-reader environments
  - Close to 100% reliability

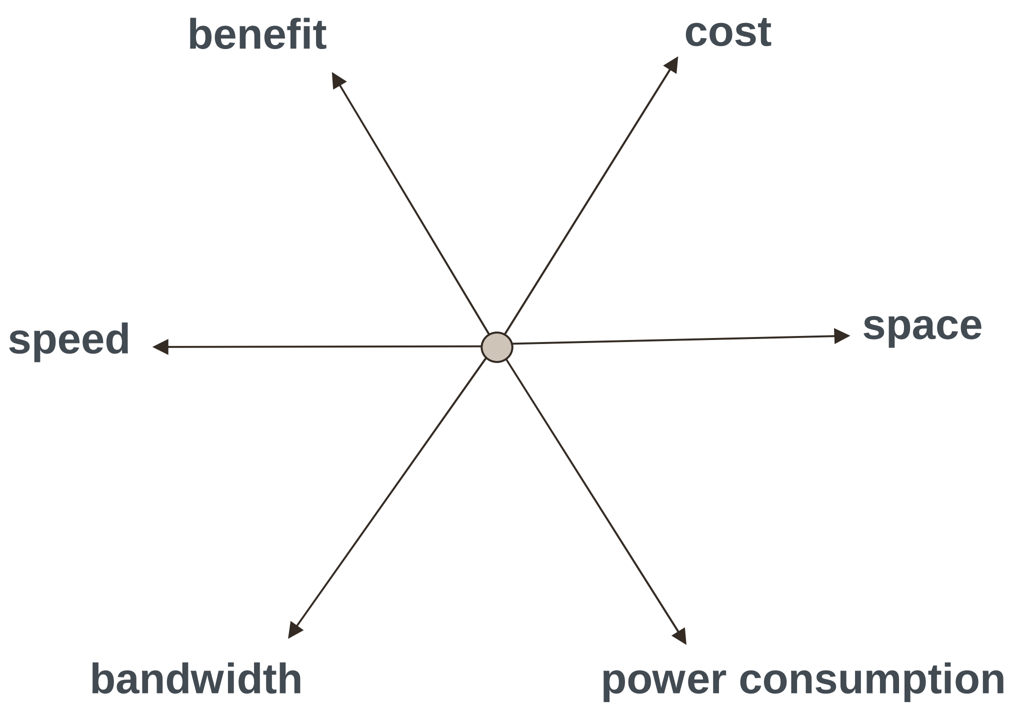
- These are very different from HF devices
  - Public transport ticketing, NFC, …
  - Much shorter operational range and more power
  - ISO 14443-x, 15693

RFID Year Zero ?

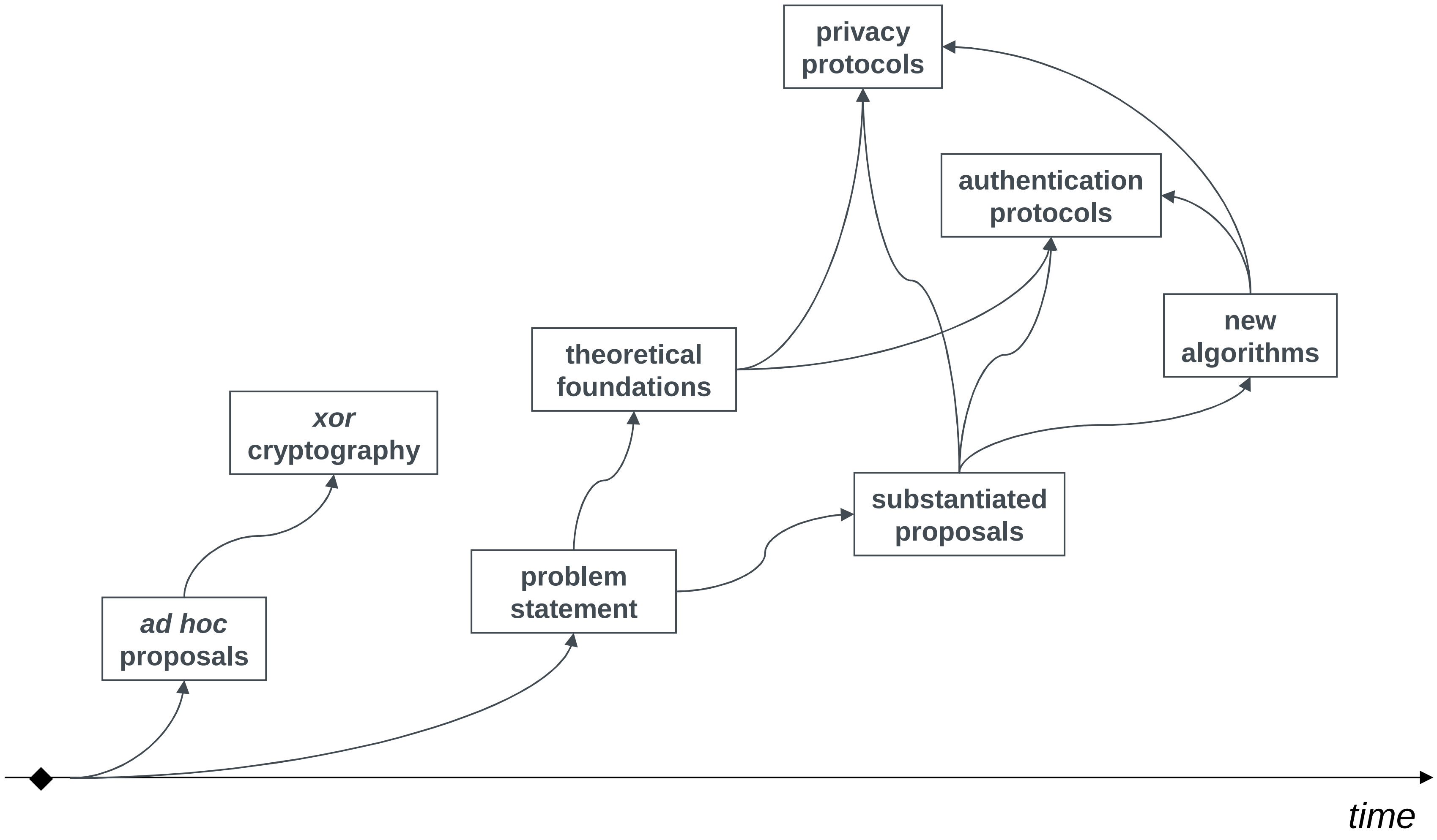
- RFID solutions have been deployed for a long time
  - Livestock monitoring
  - Access control
  - Public transport ticketing
- Academic "Year zero" for RFID tags is 1999
  - Auto-ID Center was established at MIT
    - Goal: RFID tags that can be read at a distance and yet are cheap enough to allow the tracking of individual items
  - Commercialisation continues via EPCglobal (now within GS1)
    - research continues in dedicated Auto-ID Labs
    - … and the broader academic community

RFID Tags – The Challenge

- When adding any functionality to an RFID tag, the challenge is to find the appropriate trade-off …



The Academic Path



Cryptographic Techniques

Authentication (Tag/Reader)
Algorithm-based
Hard problem-based (symmetric)
Hard problem-based (asymmetric)

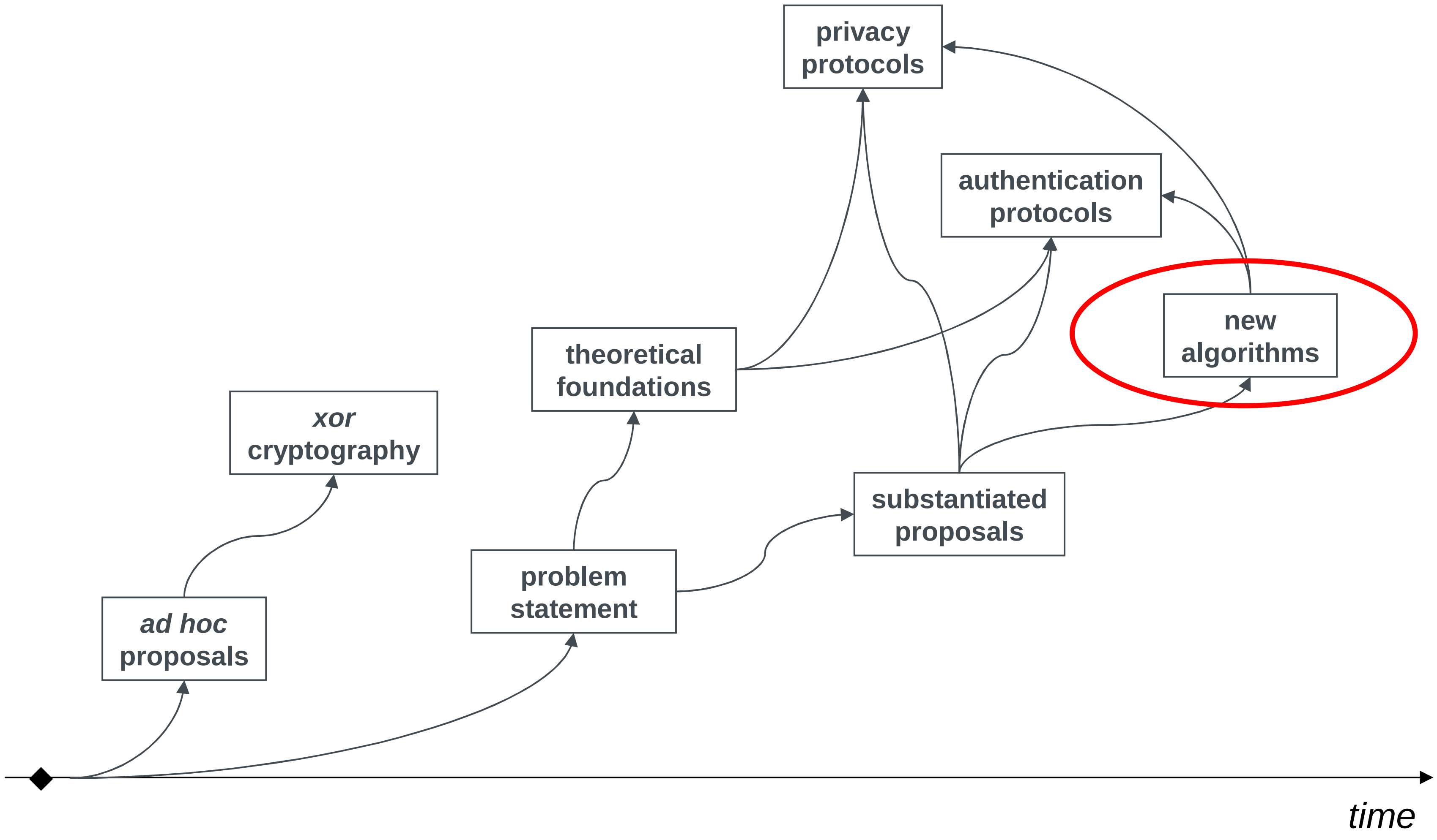
Privacy
Algorithm-based
Hard problem-based (symmetric)
Hard problem-based (asymmetric)

Protocols

Symmetric (secret key)	Asymmetric (public key)
Block ciphers	Encryption
Stream ciphers	Digital signatures
Message authentication codes	
Hash functions	

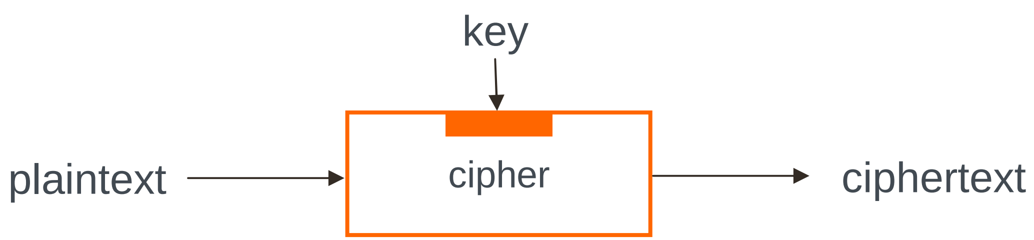
Algorithms

The Academic Path

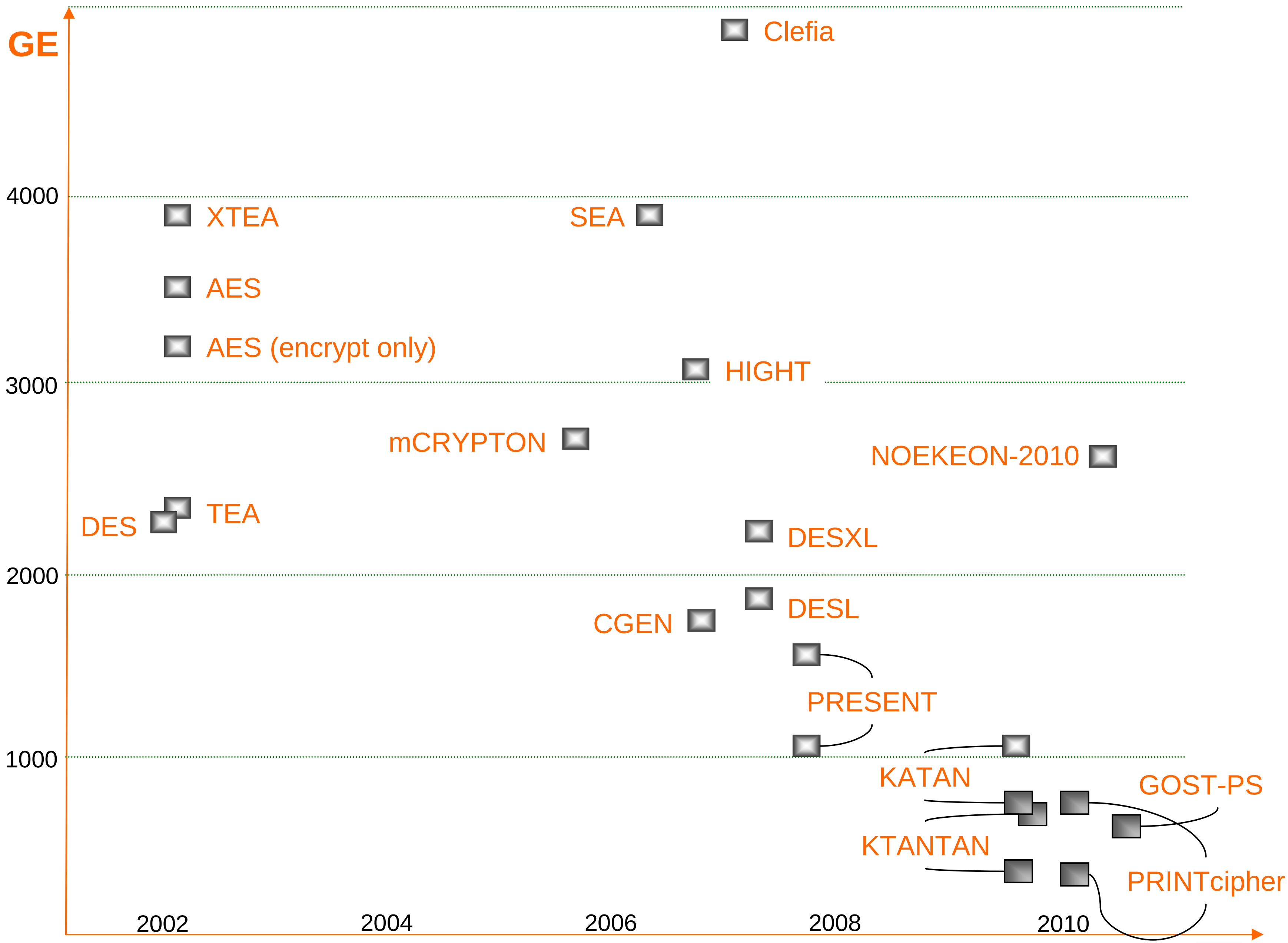


Block Ciphers

- Block ciphers provide a family of permutations under the action of a secret key
  - The important parameters are the key and the block size
  - These give fundamental space requirements



- With a block cipher we can build other components/protocols


GE
4000
3000
2000
1000
Clefia
XTEA
SEA
AES
AES (encrypt only)
HIGHT
mCRYPTON
NOEKEON-2010
DES
TEA
DESXL
CGEN
DESL
PRESENT
KATAN
GOST-PS
KTANTAN
PRINTcipher
2002
2004
2006
2008
2010

Sizes of Block Ciphers

	Block Size (bits)	**Key Size** (bits)	**Area** (GE)	**Speed** (bits/cycle)	**Efficiency** (Kbps/GE)
AES	128	128	3400	0.13	3.3
HIGHT	64	128	3048	1.88	61.8
mCRYPTON	64	128	2500	4.92	203.4
TEA	64	128	2355	1.00	42.5
DES	64	56	2300	0.44	19.1
DESXL	64	184	2168	0.44	20.3
PRESENT	64	80	1570	2.00	127.4
PRESENT	64	80	1000	0.11	11.4
KATAN64	64	80	1054	0.25	23.8
KATAN32	32	80	802	0.13	16.2
KTANTAN64	64	80	688	0.25	36.4
KTANTAN32	32	80	462	0.13	28.1
PRINTcipher	48	80	402	0.06	15.5

Academia ↔ Industry

- The search for lightweight ciphers has helped focused attention on the role of the key schedule

- Application-specific considerations can help

  - Do we need both encryption and decryption ?
  - Do we need to worry about related-key attacks ?
  - Do we need to change the key ?

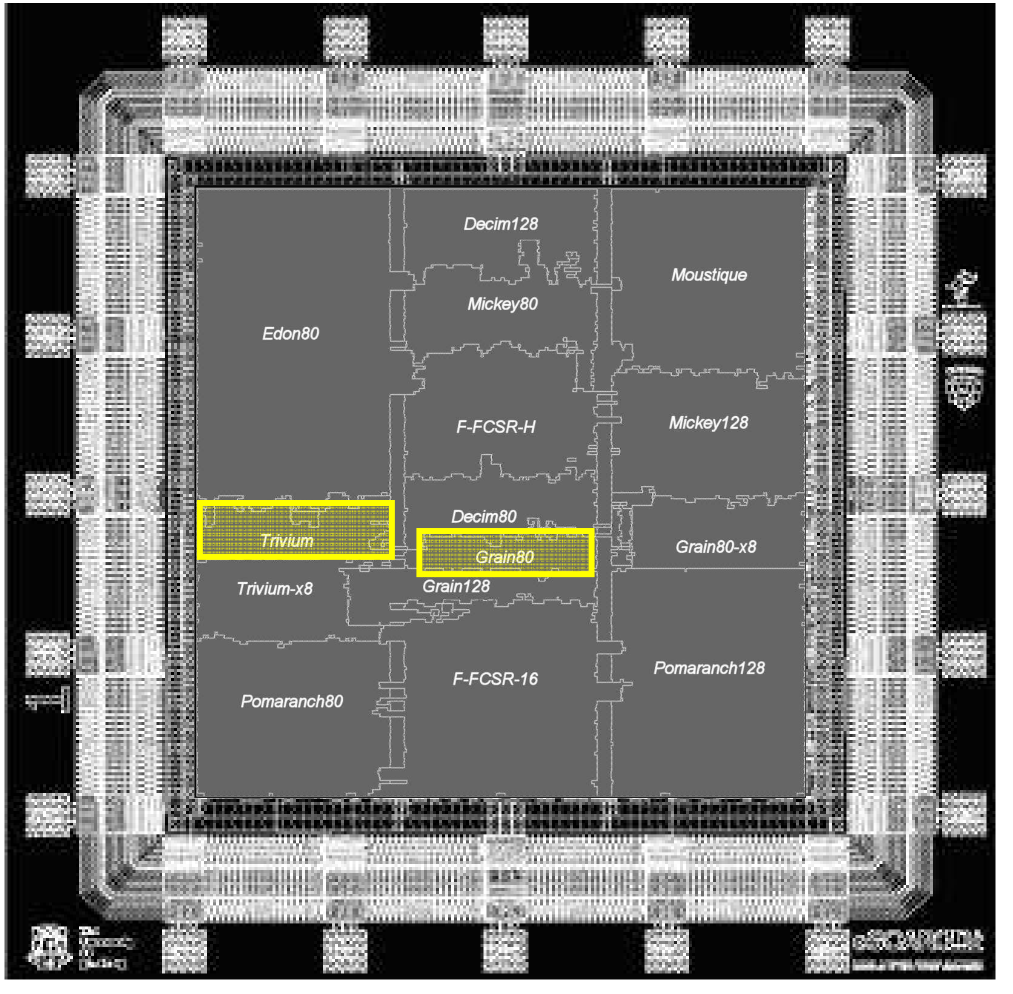
- A better understanding of security that's "fit for purpose"

- Overall, some very promising proposals

Stream Ciphers

- If you have a block cipher, you have a stream cipher, *e.g.* PRESENT in OFB or counter mode
  - But dedicated stream ciphers have the reputation of being smaller and faster than block ciphers
- One of the goals of eSTREAM was to explore this issue …
  - A project within ECRYPT Framework 6 NoE to promote dedicated stream ciphers designs
  - A particular focus on compact HW implementation
  - **Tim Good (University of Sheffield)** implemented all HW finalists

eSTREAM


Decim128
Moustique
Mickey80
Edon80
F-FCSR-H
Mickey128
Decim80
Trivium
Grain80
Grain80-x8
Trivium-x8
Grain128
F-FCSR-16
Pomaranch128
Pomaranch80

Academia ↔ Industry

- Real progress in the design of HW-oriented stream ciphers

- Before:

		Area (GE)
RC4	Widely used (*e.g.* TLS)	≈ 12000
SNOW 2.0	ISO Standardised	7000

- Now:

	Key Size (bits)	**Area** (GE)	**Speed** (bits/cycle)	**Efficiency** (Kbps/GE)
AES	128	3400	0.1	2.9
PRESENT	80	1570	2.0	127.4
Grain v1	80	1294	1.0	77.3
Grain v1 (x 8)	80	2191	8.0	365.1
Trivium	80	2580	1.0	38.8
Trivium (x 8)	80	2952	8.0	271.0

MACs and Hash

- A message authentication code is a cryptographic checksum
  - A short finger-print computed under the action of a secret key
  - Typically we would use a block cipher in an appropriate mode

- There are dedicated solutions but they are often proprietary
  - One public solution was SQUASH

- Hash functions compute a finger-print without a secret key and yet offer 1st/2nd pre-image resistance, collision-resistance, …
  - The security (should) depend on the output size
  - Hash functions today are PC-efficient but no use for tags
  - (This won't change with the NIST SHA-3 competition)

Typical Hash Functions in HW

- The hardware performance of typical hash functions

	Output Length (bits)	Area (GE)	Speed (bits/cycle)	Efficiency (Kbps/GE)
MD4	128	7350	1.1	15.0
MD5	128	8400	0.8	9.5
SHA-1	160	5527	1.5	27.1
SHA-256	256	10868	0.5	4.6

Hash Function Summary

	Output Size (bits)	Area (GE)	Speed (bits/cycle)	Efficiency (Kbps/GE)
PRESENT-based	64	1683	0.2	11.9
PRESENT-based	64	2355	4.0	169.9
PRESENT-based	128	2300	0.1	4.3
PRESENT-based	128	3962	4.0	101.0
AES-based	128	> 4400	< 0.2	< 4.5
MD4	128	7350	1.1	15.0
MD5	128	8400	0.8	9.5
SHA-1	160	5527	1.5	27.1
PRESENT-based	192	4600	0.04	0.9
PRESENT-based	192	6500	0.6	9.2
MAME	256	8100	2.7	33.3
AES-based	256	>9800	< 0.2	< 2.0
SHA-2 (256)	256	10868	0.5	4.6

Academia ↔ Industry

- Hash functions for constrained devices remain rather frustrating
  - Perhaps a better understanding of the requirements helps ?
    - Hash functions for reduced hash outputs (*e.g.* 64/80 bits) might be useful in applications that don't need collision-resistance
    - Hash functions for reduced hash outputs (*e.g.* 128 bits) can be useful in applications that need collision-resistance at low security levels
    - Quark (CHES 2010) …
- For more on hash functions see Thomas' talk !

Algorithms Summary

- There are block ciphers and stream ciphers offering 80-bit security at around 1000-2000 GE

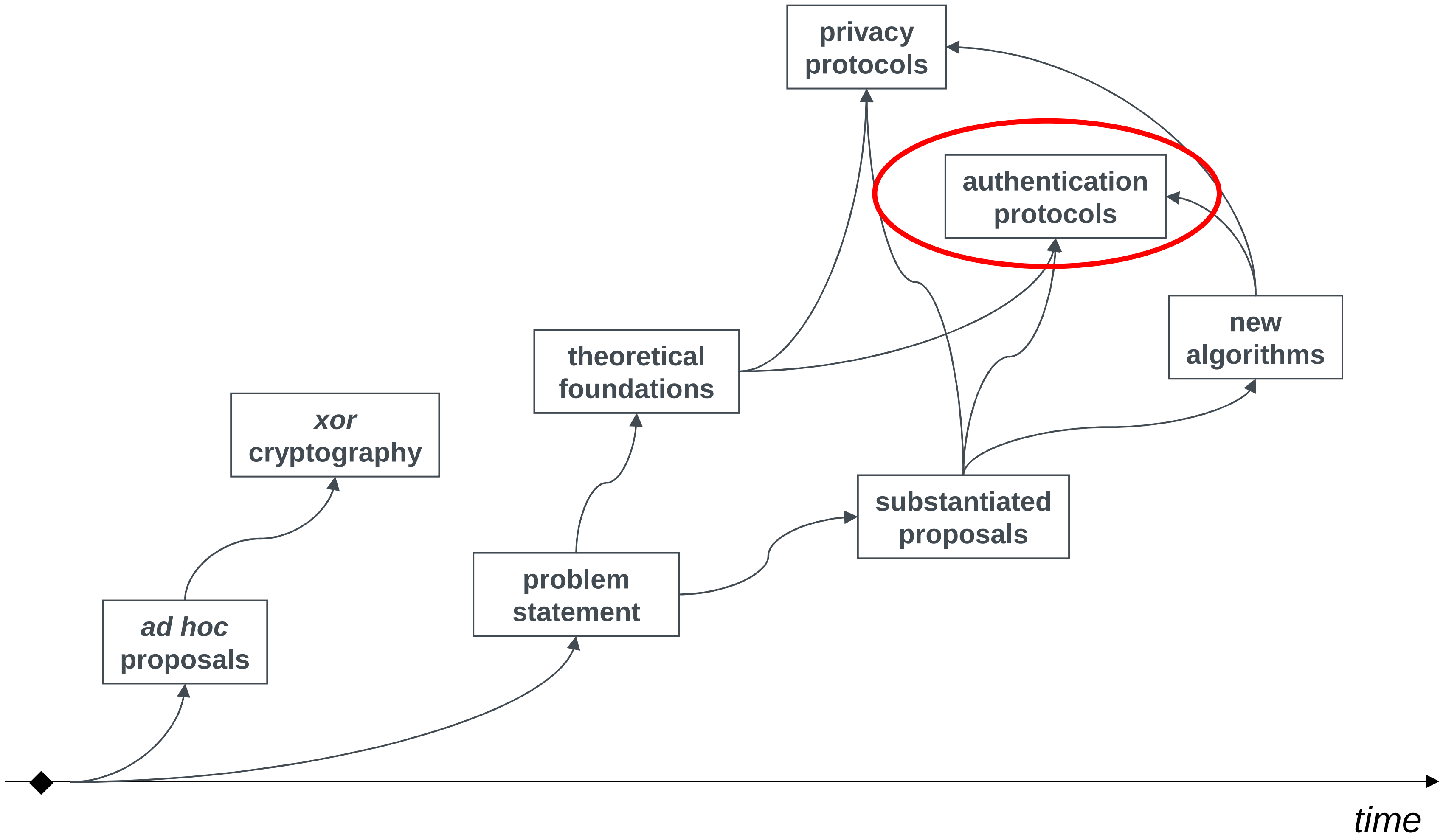
- There are MACs, but no hash functions (yet) suitable for RFID tags

  - Many RFID-privacy protocols give solutions using a hash function but these are not easy to implement on RFID tags

- There are no PK encryption or signature schemes suitable for cheap UHF passive tags

  - RSA is far too large and smallest EC engines require around 10000 GE
  - The only (published) NTRU encryption implementation has 3000 GE but offers low security and requires 30000 cycles

The Academic Path



Tag Authentication

- Tag authentication is seen as a valuable technique in the fight against product counterfeiting
  - 11% of global pharmaceutical commerce is counterfeit ($39 billion) *[Bridge]*
- To use tags for anti-counterfeiting we need to show the tag is authentic
  - Network-based: on-line verification to identify odd behaviour
  - Static authentication: tags carry a digital signature of (say) the TID
  - Dynamic authentication: tags perform some cryptography
- Dynamic authentication is the appropriate security solution
  - Both symmetric and asymmetric dynamic authentication is possible on cheap UHF tags

Cryptographic Techniques

Authentication (Tag/Reader)
Algorithm-based
Hard problem-based (symmetric)
Hard problem-based (asymmetric)

Privacy
Algorithm-based
Hard problem-based (symmetric)
Hard problem-based (asymmetric)

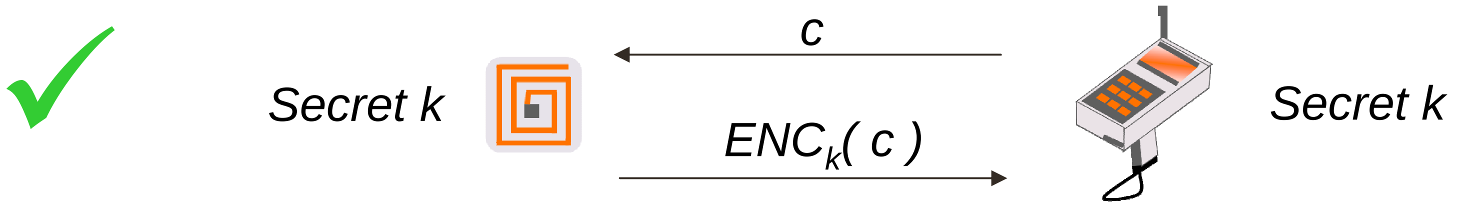
Protocols

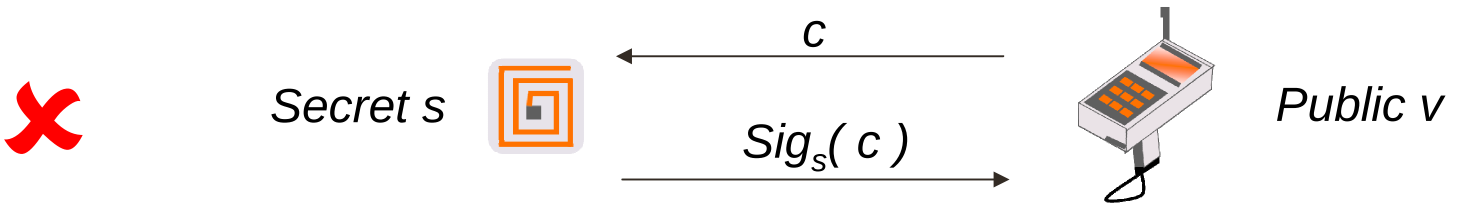
Symmetric (secret key)	Asymmetric (public key)
Block ciphers	Encryption
Stream ciphers	Digital signatures
Message Authentication Codes	
Hash functions	

Algorithms

Algorithm-based Tag Authentication

- Device authentication via a challenge-response protocol





Cryptographic Techniques

Authentication (Tag/Reader)
Algorithm-based
Hard problem-based (symmetric)
Hard problem-based (asymmetric)

Privacy
Algorithm-based
Hard problem-based (symmetric)
Hard problem-based (asymmetric)

Protocols

Symmetric (secret key)	Asymmetric (public key)
Block ciphers	Encryption
Stream ciphers	Digital signatures
Message Authentication Codes	
Hash functions	

Algorithms

Cryptographic Techniques

Authentication (Tag/Reader)
Algorithm-based
Hard problem-based (symmetric)
Hard problem-based (asymmetric)

Privacy
Algorithm-based
Hard problem-based (symmetric)
Hard problem-based (asymmetric)

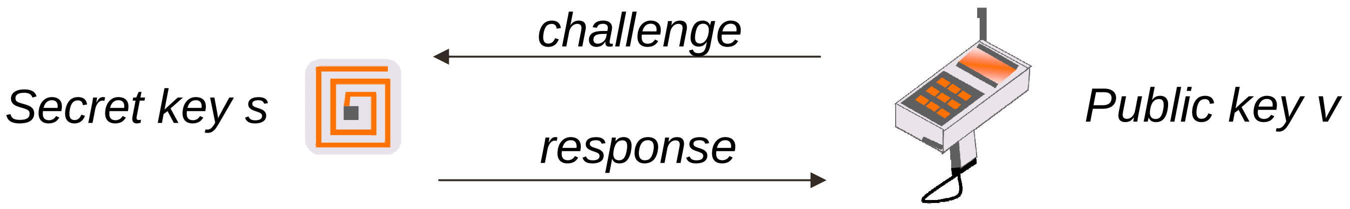
Protocols

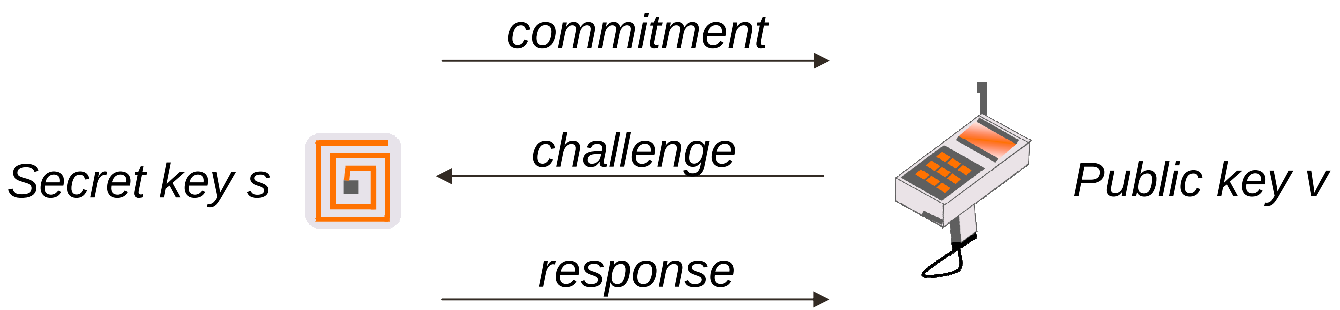
Symmetric (secret key)	Asymmetric (public key)
Block ciphers	Encryption
Stream ciphers	Digital signatures
Message Authentication Codes	
Hash functions	

Algorithms

CRR

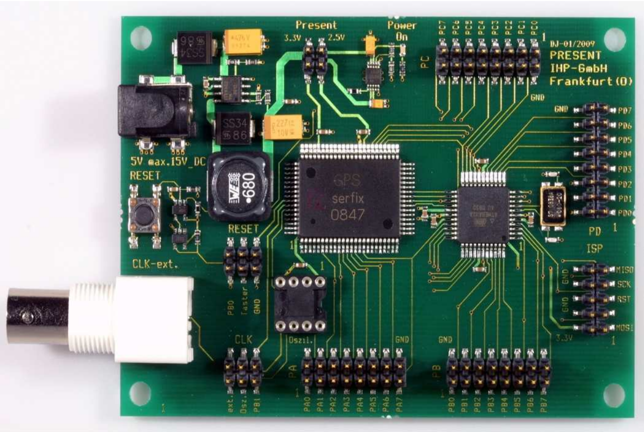
- Tag authentication via commitment-challenge-response (CCR)





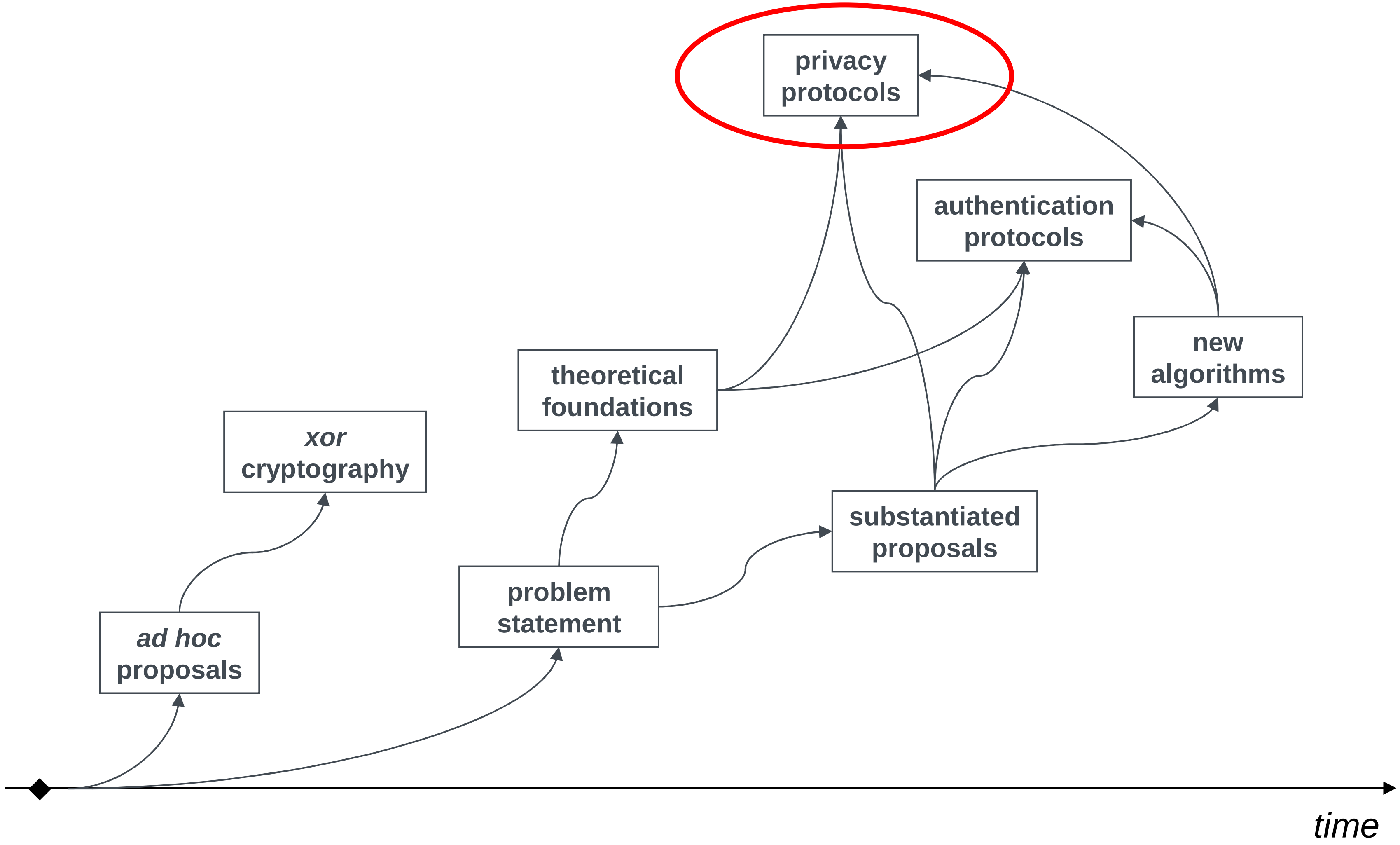
cryptoGPS

- Due to Girault, Poupard, and Stern
  - ISO/IEC 9798-5, CD ISO 29192
  - Widely studied and implemented



- Cryptographic computation + supporting cryptographic modules fabricated in silicon (uses PRESENT for one component)
  - Asymmetric tag authentication: 2876 GE and 724 cycles
  - In fact PRESENT dominates the implementation (1751 GE)
  - See proceedings of *ICISC 2009*, LNCS 5984

The Academic Path



Protocols for Privacy

- Currently mixed success but, depending on the goals, there are some solutions available (also physical solutions and helper-devices)
- Rather a confusing mix of proposals early on …

Protocols for Privacy

- Many proposals require the use of a hash function, however these are difficult to implement in practice

- However some recent proposals satisfy both new privacy models and practical constraints

  - *e.g.* PEPS which provides *almost-forward-private* authentication
    - Intended to be built around a stream cipher with IV for which we know we have good lightweight proposals, *e.g.* Grain v1.0

- The field is maturing quickly, see Prof. Deng's presentation!

The Academic Side – 10 years on

- Algorithms
  - For symmetric algorithms we're in good shape; we're approaching theoretical limits, several schemes are very promising
  - There are still no compact public-key encryption or signature algorithms
- Protocols
  - Dynamic tag authentication (secret- or public-key) is entirely feasible
  - Solutions for privacy not so well developed, but the area is promising

The Industry Side – 10 years on

- The UHF tag industry has not (yet) taken off as expected
- Many high-profile trials, but the financial crisis came at a bad time
- Deployments might take place in different ways; pallet, case, and item
  - The real interest is in making the item-level tag economical
- However the market for UHF tags continues to grow
  - Though the 5¢ UHF tag still appears to remain elusive

Looking Forwards

- Will we see lightweight cryptography deployed ?
  - Perhaps a good solution for dynamic tag authentication (anti-cloning), though balancing the different costs of deployment will remain a big issue
- An open question: is the RFID/cost issue the right way around ?
  - RFID tags are much more than easy-to-use barcodes
    - We can write/read with them, we can authenticate them (cryptographically), …
  - The infrastructure investment might be large for any RFID deployment
    - Instead of avoiding functionality on the tag, would adding functionality help provide a better case for deployment ?

- Thank you for your attention !