

Security outside the black-box model Countermeasures and Challenges

Ventzi Nikov

NXP Semiconductors, Belgium

CARDIS 2016,

November 8th 2016

Disclaimer

"The Moral Character of Cryptographic Work", Phil Rogaway, 2015.



- This talk is addressed to the cryptographic and security community - my community and the words "we" and "our" should be so interpreted.
- I apologize in advance if I offend anyone with any of my comments; nothing of the sort is my intent.

Any views, opinions, findings, conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the NXP Semiconductors.

Introduction

Intro

An observation: A clear **division** - theoreticians vs. practitioners in the community.

Which hat:  or  should I use?

Black-box crypto - **fundamental** or applied research?

Outside the black-box model - fundamental or **applied** research?

Unprotected Implementations

Optimized on:
performance and throughput, latency, area (GE in HW, ROM and RAM in SW), power, energy, etc.

HW Implementations:

- Different CMOS libraries - **incomparable** GE figures.
- Registers vs. latches, hard-coding the key, etc. - to reduce area
- AES vs. a lightweight cipher: only encryption, but what about the decryption overhead?
What if support of more key sizes has to be added?

Atomic-AES	ED	STM 90nm	2645
		STM 65nm	2976
8-bit Serial	E	UMC 180nm	2400

SW Implementations:

4, 8, 16, 32 to 64 bit CPUs; cache vs. no cache; higher level language like C/C++ or Assembly; etc.

Unprotected Implementations

Is there a more **fair way to compare** implementations?

The industry uses mainly **standardized ciphers** and in fact only a **few of them**.

Do we need all these similar designs? How can one sieve the best?

Interoperability and **support** are harder problems than the efforts to standardize and adopt new cipher.

Protecting crypto HW implementations in the grey-box model

MPC and SCA countermeasures

Secret Sharing, Proactive Secret Sharing and Multi Party Computation:
t-bounded **passive adversary**, over any finite field.

ISW “Private circuits” (Crypto 2003) and the analogy to MPC in HW – GF(2)

The “**temporal**” separation simulating the MPC approach (SW friendly – GF(2ⁿ)),
“Provably secure higher-order masking of AES”, Rivain and Prouff, CHES 2010

Algorithm 1 SecMult - d th-order secure multiplication over \mathbb{F}_{2^n}

INPUT: shares a_i satisfying $\bigoplus_i a_i = a$, shares b_i satisfying $\bigoplus_i b_i = b$

OUTPUT: shares c_i satisfying $\bigoplus_i c_i = ab$

1. **for** $i = 0$ **to** d **do**
 2. **for** $j = i + 1$ **to** d **do**
 3. $r_{i,j} \leftarrow \text{rand}(n)$
 4. $r_{j,i} \leftarrow (r_{i,j} \oplus a_i b_j) \oplus a_j b_i$
 5. **for** $i = 0$ **to** d **do**
 6. $c_i \leftarrow a_i b_i$
 7. **for** $j = 0$ **to** d , $j \neq i$ **do** $c_i \leftarrow c_i \oplus r_{i,j}$
-

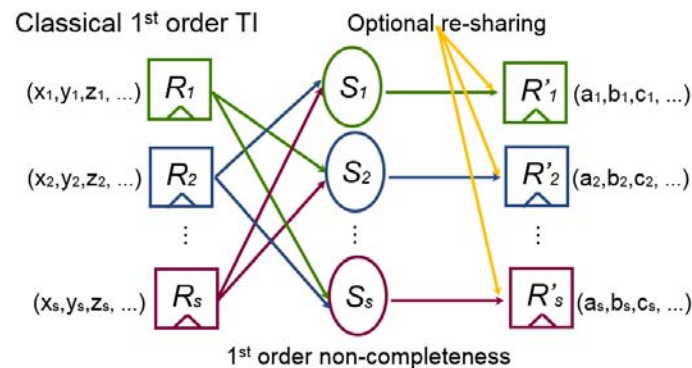
Passive attacks – SCA countermeasures

ISW “Private circuits” (Crypto 2003) and the analogy with MPC in HW

The “temporal” separation simulating the MPC approach (SW friendly)
“Provably secure higher-order masking of AES”, Rivain and Prouff, CHES 2010

The “spatial” separation tweaking the MPC approach into HW.

- “classic” deg^*d+1 TI - *“Threshold Implementations against Side-Channel Attacks and Glitches”, Nikova et al., ICICS 2006;*
“Higher-order threshold implementations”, Bilgin et al., Asiacrypt 2014



Passive attacks – SCA countermeasures

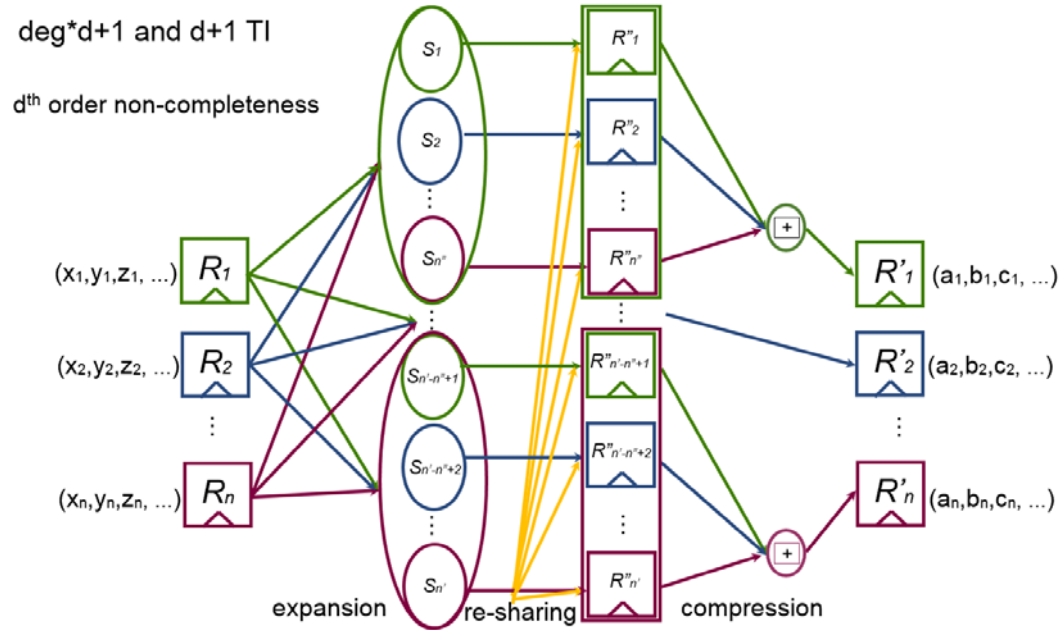
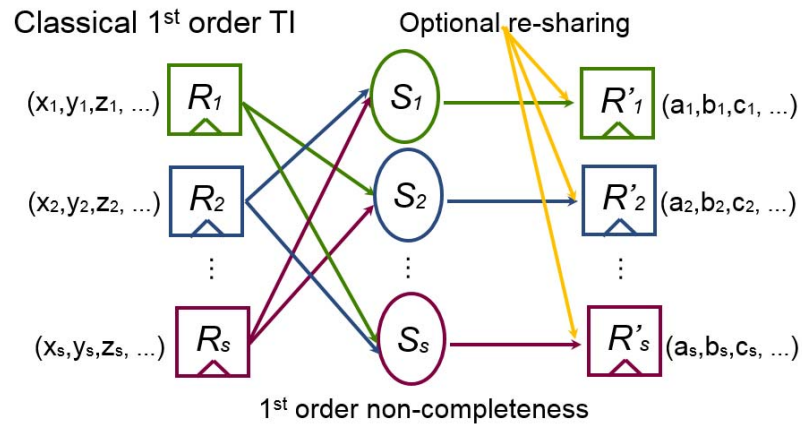
ISW “Private circuits” (Crypto 2003) and the analogy to MPC in HW

The “temporal” separation simulating the MPC approach (SW friendly)

“Provably secure higher-order masking of AES”, Rivain and Prouff, CHES 2010

The “spatial” separation tweaking the MPC approach into HW.

- “classic” $\deg \cdot d + 1$ TI - *“Threshold Implementations against Side-Channel Attacks and Glitches”, Nikova et al., ICICS 2006;*
“Higher-order threshold implementations”, Bilgin et al., Asiacrypt 2014
- $d + 1$ TI or CMS –
“Consolidating masking schemes”, Reparaz et al., Crypto 2015



Passive attacks – SCA countermeasures

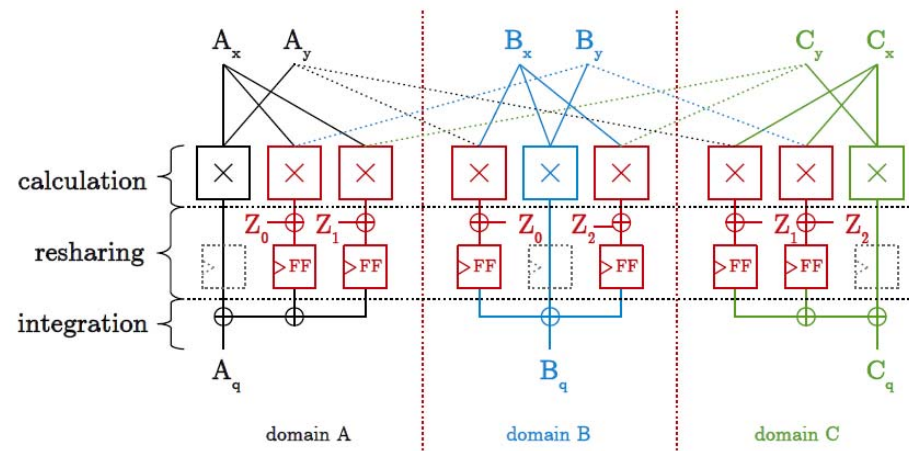
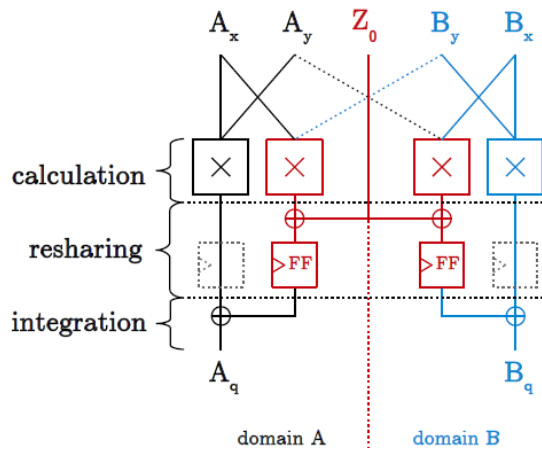
ISW “Private circuits” (Crypto 2003) and the analogy to MPC in HW

The "temporal" separation simulating the MPC approach (SW friendly)
“Provably secure higher-order masking of AES”, Rivain and Prouff, CHES 2010

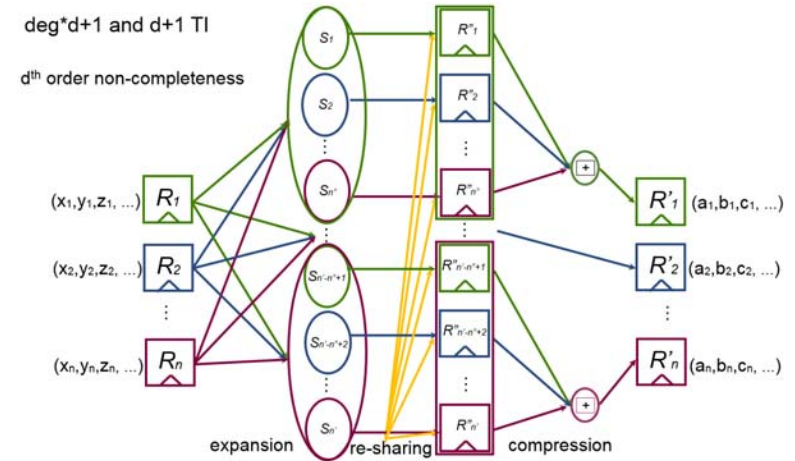
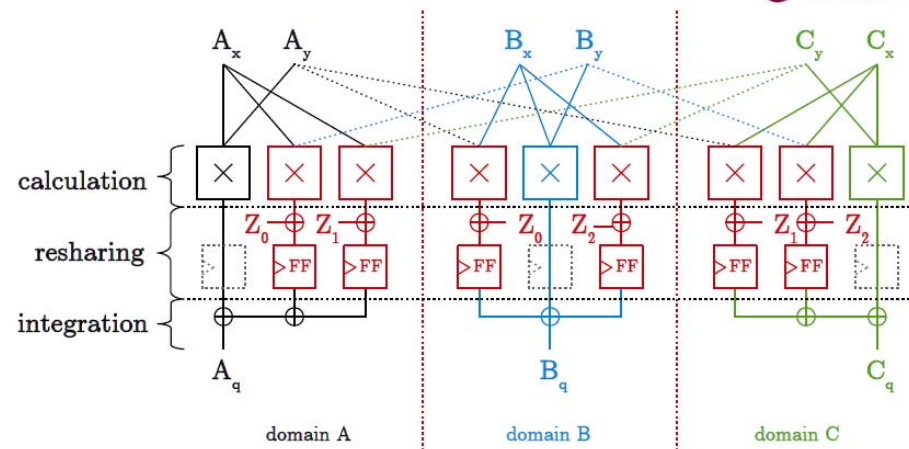
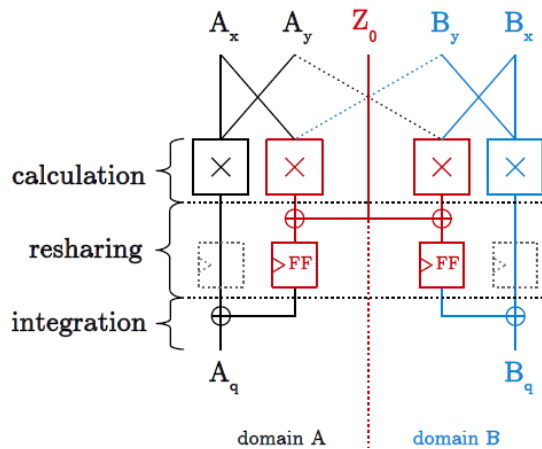
The “spatial” separation tweaking the MPC approach into HW.

- “classic” $\text{deg} \cdot d + 1$ TI - *“Threshold Implementations against Side-Channel Attacks and Glitches”, Nikova et al., ICICS 2006 ;*
“Higher-order threshold implementations “, Bilgin et al., Asiacrypt 2014
- $d + 1$ TI - *“Consolidating masking schemes”, Reparaz et al., Crypto 2015*
- DOM 2016
“Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order”, Gross et al., e-print Archive 2016/486

DOM 1st and 2nd order Multiplier



DOM 1st and 2nd order Multiplier



Relations between: ISW, TI, CMS, DOM
Where to draw the line?

Crypto in HW - the grey-box model

Passive attacks – SCA countermeasures

ISW “Private circuits” (Crypto 2003) and the analogy to MPC in HW

The "temporal" separation simulating the MPC approach (SW friendly)
“Provably secure higher-order masking of AES”, Rivain and Prouff, CHES 2010

The “spatial” separation tweaking the MPC approach into HW.

- “classic” $\deg \cdot d + 1$ TI - *“Threshold Implementations against Side-Channel Attacks and Glitches”, Nikova et al., ICICS 2006 ;*
“Higher-order threshold implementations”, Bilgin et al., Asiacrypt 2014
- $d + 1$ TI - *“Consolidating masking schemes”, Reparaz et al., Crypto 2015*
- DOM 2016 - *“Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order”, Gross et al., e-print Archive 2016/486*

Where to draw the line?

Which solutions are “generic”?

MPC vs. SCA countermeasures

In HW SCA countermeasures the “cost” comes from

- The number of shares (also intermediate) to be stored in registers == storage cost of MPC
- The cost of the circuit gadgets (but wiring is free) == computational cost of MPC
- Randomness - a common open problem for both MPC and SCA countermeasures
- Performance - in HW many operations are in parallel, still registers are used for separation <> to the communication cost of MPC;

In MPC the emphasis is on optimizing the protocol overhead (i.e. minimizing the data exchanged), while in HW more important is the required area.

The objectives to obtain efficient MPC over a network and in HW are quite different.

Passive attacks – challenges

Security

- Dynamic or Static Power Leaks more
“Side-Channel Leakage through Static Power - Should We Care about in Practice?”,
Moradi, CHES 2014.
- Working hypothesis should be tested using observations and experiments
- Many publications do not offer any implementation or evaluation
 - Other use only 1-2M traces
 - Some (very few) use 20-100M traces

Passive attacks – challenges

- **Randomness** - *“Randomness Complexity of Private Circuits for Multiplication”, Belaid et al., Eurocrypt 2016.*
Open problems: secure re-sharing, reduce randomness, quality requirements.
However in practice simpler solutions help e.g. the approach of “borrowing” random bits *“On non-uniformity in threshold schemes”, Daemen, 2016.*
- **Performance** - is not an issue but still can be improved.

Passive attacks – challenges

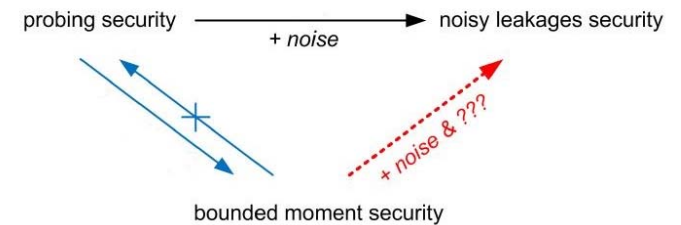
- **Latency** - especially for memory encryption posed as an open problem
“Side-Channel Analysis Protection and Low-Latency in Action – case study of PRINCE and Midori”, Moradi and Schneider, Asiacrypt 2016.
- **Area** - not a big problem, however it always will be an issue
 - Ad hock (“hiding”) solutions will always be cheaper (less area).
- **Power** - can be a problem in certain cases (and energy too).

Passive attacks – models

SCA models commonly used

- t-wire probing: static, adaptive, random, etc.
 - Strong non-interference - enables compositional verification “*Strong non-interference and type-directed higher-order masking*”, Barthe et al., CCS 2016.
 - continuous t-wire adversaries
- > Simple but strong adversary models
- A more realistic - noisy leakage model: Duc et al., Eurocrypt 2014, 2015
 - Those models may serve well for SW but do they reflect the HW specifics?
A step closer “*Parallel Implementations of Masking Schemes and the Bounded Moment Leakage Model*”, Barthe et al., e-print Archive 2016/912

Hence we still need realistic adversary models.



Active attacks – FA

In addition to SCA however we always need FA protection

“Trivial” countermeasures:

- Duplication - spatial or temporal
- Concurrent error-detecting or error-correcting codes
- Kind of multi-party secure against **active adversaries**
- ... anything else

Therefore to find sound FA countermeasures is still an open problem.

Lack of methods and more important lack of models

Combined attacks – FA & SCA

Even a harder open problem: protection against a combination of SCA and FA

- Still far from finding sound solutions – a step forward:
“ParTI - Towards Combined Hardware Countermeasures against Side-Channel and Fault-Injection Attacks”, Schneider et al., Crypto 2016.

What about other HW effects and attacks?

- **coupling effect** - a step forward: *“Does Coupling Affect the Security of Masked Implementations?”*, De Cnudde et al., e-print Archive 2016
- **reverse-engineering** - allows “cloning” and ... is transforming the HW from the grey-box model closer to the white-box model

LR crypto in HW and SW
in the grey-box model

LR crypto in HW and SW

Leakage Resilient Crypto - begun eight years ago as fundamental research and is still mostly theoretical

Are there ways to turn this into applied research?

Few obstacles

- How provably and efficiently to protect stateless symmetric cryptographic primitives such as block ciphers. Is re-keying the only option?
- Uses non-standard ways to achieve LR thus hardly adoptable in industry

A step closer is

"Unknown-Input Attacks in the Parallel Setting: Improving the Security and Performances of the CHES 2012 Leakage-Resilient PRF", Medwed et al., Asiacrypt 2016

Still a long way to go

Protecting crypto SW implementations
in both grey and white-box models

Crypto in SW - the grey-box model

Passive SCA and countermeasures

- The “temporal” separation simulating the MPC approach (SW friendly)
“Provably secure higher-order masking of AES”, Rivain and Prouff, CHES 2010
- Series of papers: Carlet et al. [CGPQR12], Coron et al. [CRV14], Carlet et al. [CPRR15]
gradually improving security and performance
- Secure computation of an S-box is equivalent to Secure evaluation of a Polynomial in $GF(2^n)$
- TI can be used in a bit-sliced manner
- Still they all might be too slow and require too much randomness (in SW this can be an issue)
- The adversary models are stronger in SW than in HW

For FA and combined attacks - still open problems as for the HW
in fact even worse since the SW implementations are even more vulnerable

Crypto in SW - the white-box model

White-box crypto – started fifteen years ago as applied research.

Is there a way to become fundamental?

The known "practical schemes" are broadly used and ... all are broken.
Even with mathematical (or SW) only attacks

In fact those schemes are broken in all possible models - grey (DPA & FA) and white (DCA)
"Differential Computation Analysis: Hiding your White-Box Designs is Not Enough", Bos et al., CHES 2016; "Unboxing the white-box: Practical attacks against obfuscated ciphers", Sanfelix et al., BlackHat Europe 2015; "White-box cryptography in the gray box - a hardware implementation and its side channels", Sasdrich et al., FSE 2016.

Why did this happen?

“Theory” is still far from reality, instead “SW obfuscation” is used.
Reverse-engineering is a big problem. The indistinguishable obfuscation (iO) – might become a theoretical solution but what does it provide?

Secure execution = platform security

Protecting any SW execution in the white-box model

Is this Research or Advanced Development?

Protecting against SW only attacks

- SW alone is not enough: how can HW help - SE, TPM, TEE, MPU, etc.
Only few publications:
"SMART: Secure and Minimal Architecture for (Establishing Dynamic) Root of Trust", Eldefrawy et al., NDSS 2012; *"SANCUS: Low-cost trustworthy extensible networked devices with a zero-software Trusted Computing Base"*, Noorman et al., USENIX 2013
- SGX – revealed to public in 2013

Attacker community – hackers; Reverse-engineering is a big problem

Protecting against physical attacks

- Using trivial techniques (like double execution) against FA
- Noise and balancing against DPA, SCA countermeasures in certain parts of ALU

Protecting any platform in the white-box model

Several CPUs in parallel - a SoC

- How TPM or SE can help protecting the SW execution on different CPUs?
 - What about protecting the memories and the busses?
 - What about the external interfaces and sensors - the real physical input to the system?
-
- Does it make sense to secure a crypto coprocessor against SCA up to few M traces?

Protecting any platform in the white-box model

Several CPUs in parallel - a SoC

- How TPM or SE can help protecting the SW execution on different CPUs?
- What about protecting the memories and the busses?
- What about the external interfaces and sensors - the real physical input to the system?

- Does it make sense to secure a crypto coprocessor against SCA up to few M traces?
- When the platform is insecure e.g. SW hacked in 5 sec?



Security and its cost

Security comes with additional overhead == cost

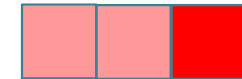
- Who is willing to pay the bill for security?
- Industry or the end user - what level is affordable?

First DDoS (Distributed denial-of-service) attacks using IoT devices 21.10.2016

- “If we can't stop the vulnerabilities getting into people's homes in the first place, can we at least fix them afterwards?”
- But how to repair those compromised devices?
- Who is responsible for the maintenance/updates and who will pay?

Where we stand

- Protecting crypto HW implementations in the grey-box model
 - Side channel attacks, Fault attacks, Combined attacks, Coupling, Reverse-engineering
- LR crypto in HW and SW in the grey-box model
- Protecting crypto SW implementations in the grey-box model
 - Side channel attacks, Fault attacks, Combined attacks
- Protecting crypto SW implementations in the white-box model
 - Grey-box attacks, White-box attacks, Reverse-engineering
- Protecting any SW execution in the white-box model
 - SW attacks, Physical attacks, Reverse-engineering
- Protecting any platform in the white-box model
 - SW attacks, Physical attacks, Reverse-engineering



Final words

We are facing more, bigger and complex challenges.

However we are progressing too slow with countermeasures.
I feel we failed to scale to today's needs.

Are we focusing on the important problems?

Security > Crypto > Math

- Outside the black-box proper modelling of the adversary is paramount
- Progress possible only by working together: Theoreticians and Practitioners
- We need both fundamental and applied research
- Our understanding does not scale well in more complex systems

Finite vs. infinite games – what type of games crypto and security are?

Thank you!

