RTCPS call 2014

SECODE

Progress in year 1

CHIST-ERA seminar , Brussels

March 2017

Pr. Jean-Luc Danger Télécom ParisTech/LTCI

SECODE GOALS

Secure Codes to thwart Cyber-physical Attacks

- To specify and design **error correction codes** suitable for an efficient protection of sensitive information in the context of Internet of Things (IoT) and connected objects.

- The codes can mitigate:
  - **passive attacks**, like memory disclosure, and
  - **active attacks**, like stack smashing.

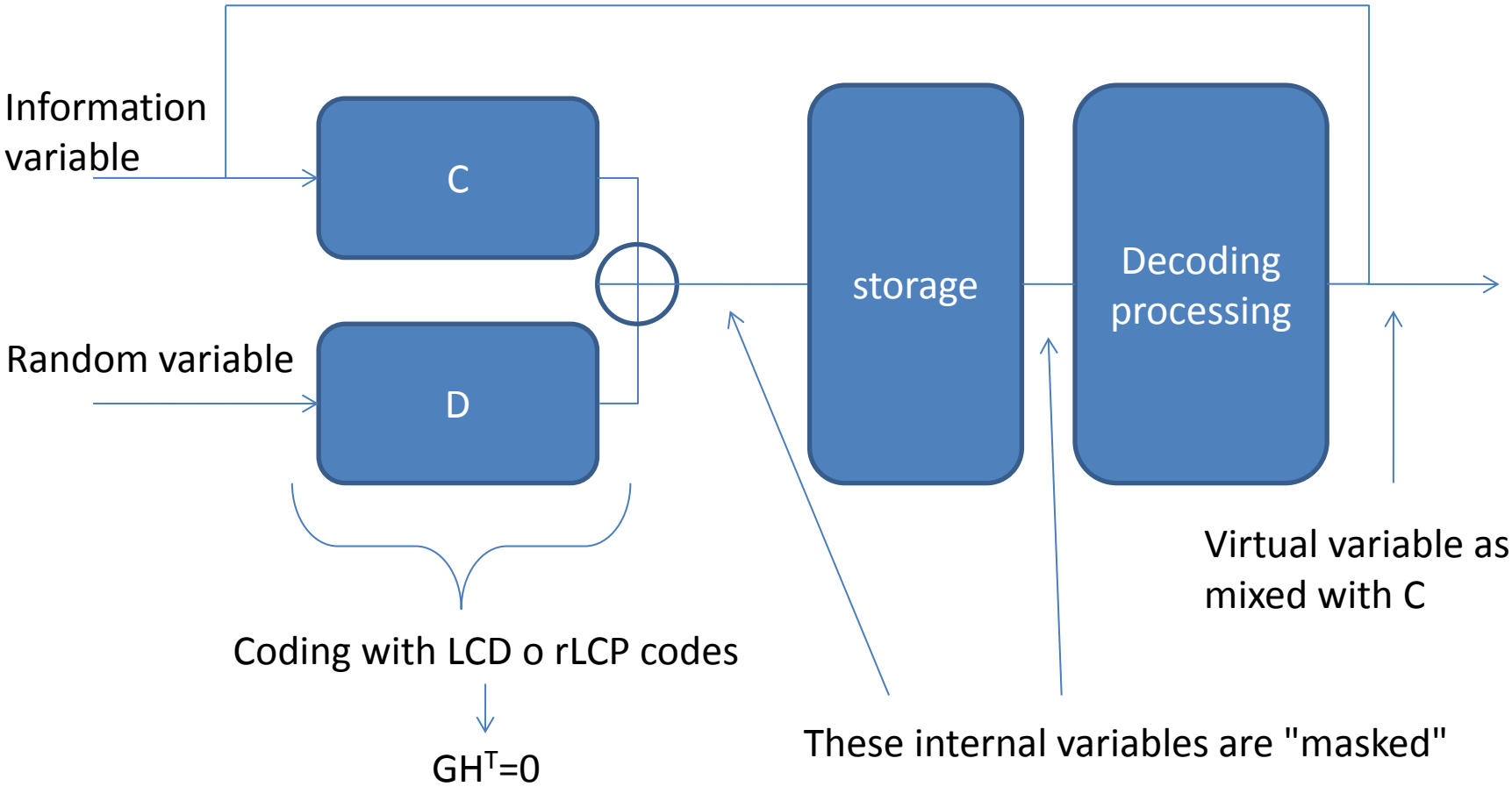
SECODE partners

LTCI

SECODE challenges

- **Code Theory:**
  - **Design of "Linear Complementary Dual" LCD codes**
    - which are “Generalized Quasi Cyclic” (GQC).
    - Relations between LCD codes and AG codes (codes defined by an algebraic curve).
- **Code implementation:**
  - **Security parameters against Physical attacks:**
    - Masking against Side channel attacks
    - Detection of faults.
  - **Cyber physical protected platform:**
    - Modified LLVM embedding protections based on codes.
    - Protected cryptoprocessor with codes for masking and fault detection.

Use of LCD/LCP codes: big picture



Code Theory

- **1. Structure and performance of generalized quasi-cyclic codes** (Partners involved: Güneri, Özbudak, Özkaya, P. Solé): Algebraic and concatenated structures of generalized quasi-cyclic (GQC) codes are obtained, a trace representation and a minimum distance bound are presented, criteria for LCD GQC's are obtained and existence of asymptotically good LCD GQC codes is proved.

Resulting paper has been submitted to the journal: Finite Fields and Their Applications

- **2. LCD AG Codes** (Partners involved: Mesnager): LCD codes in Algebraic Geometry (AG) codes are investigated. Particularly, LCD codes coming from elliptic, hyperelliptic and the Hermitian curves are studied. As a result, some MDS and optimal LCD codes are obtained.

Resulting paper (joint with C. Tang and Y. Qi) has been submitted to the journal: IEEE Transactions on Information Theory.

Code Theory

- **3. On LCD multinegacirculant codes (Partners involved: Güneri, Özkaya (project post-doc), Solé):** One-generator negacirculant LCD codes are studied for index greater than or equal to 2, good LCD codes of index 2 are obtained, enumeration results are obtained and existence of LCD multinegacirculant codes reaching a modified Gilbert-Varshamov bound is settled for all indices.

Resulting paper (joint with A. Alahmadi and H. Shoaib) has been submitted to the journal: Cryptography and Communications.

- **4. A concatenated type construction of LCD and LCP codes (Partners involved: Carlet, Güneri, Özbudak, Solé):** A concatenated type construction of LCD and LCP codes are obtained, starting with such codes over an extension field and obtaining new such codes over a smaller finite field. This is an instance of a "secondary construction" of LCD and LCP codes.

This work started in Marseille-Luminy in March 2016 when the partners involved met for a concentrated research for a week and it is still in progress.

Code Implementation : security parameters

- **LCD and LCP codes for masking, security parameters (Partners involved: all members of SECODE from all work packages):** Specification of LCD and LCP codes needed for extending inner product masking and orthogonal direct sum masking (ODSM) by the use of nontrivial LCD/LCP codes.

1 Masking at word and bit bit levels: comparaison of metrics

1.1 Unification of inner product masking and ODSM

Inner product masking ([1]) can be viewed as two complementary codes C and D (as used in ODSM[1]) such that $C \oplus D = \mathbb{F}_{2^k}^n$, where the generating matrices M_C and M_D of C and D are:

$$M_C = \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

$$M_D = \begin{pmatrix} L_2 & L_2 & 0 & \dots & 0 \\ L_3 & 0 & L_3 & \dots & 0 \\ \vdots & 0 & 0 & \ddots & 0 \\ L_n & 0 & 0 & \dots & L_n \end{pmatrix}.$$

Code Implementation : security parameters

$$M_D = \begin{pmatrix} L_2 & L_2 & 0 & \dots & 0 \\ L_3 & 0 & L_3 & \dots & 0 \\ \vdots & 0 & 0 & \ddots & 0 \\ L_n & 0 & 0 & \dots & L_n \end{pmatrix}$$

- probing security: dual distance of M_D (where L_i are coef in F_{2^k})
  - With this form: dual distance is always $n - 1$ ✓

Code Implementation : security parameters

$$M_D = \begin{pmatrix} L_2 & L_2 & 0 & \dots & 0 \\ L_3 & 0 & L_3 & \dots & 0 \\ \vdots & 0 & 0 & \ddots & 0 \\ L_n & 0 & 0 & \dots & L_n \end{pmatrix}$$

Expended code from F_{2^k} to F_2 ⟶ New $[nk, (n-1)k]$ matrix Called M'_d

- Look at the expended code from F_{2^k} to F_2 (each L_i becomes $[k, k]$ matrix representing the linear application of the multiplication by L_i)
- Under some physical & implementation assumption, the probing security can be improved from n-1 to the dual distance of M'_d
  - The dual distance of M'_d is higher or equal to the one of M_d ✓
  - These assumptions can be hard to achieve ine practice ✗

Code Implementation : modified LLVM

Implementation of compiler-based transformations

- Implementation done inside *LLVM*
- Automation of the encoding process (no source or assembly editing)
- Transparent for the user (just compile your code)
- Control over low-level instructions before binary generation

***LLVM* in brief**

- An open-source, modular and reusable compiler infrastructure
- Source-independent transformations (C, C++, Fortran, …)
- Target-independent transformations (ARM, x86, PowerPC, …)
- Custom transformations and optimizations are easily addable

Code Implementation : modified LLVM

An easy scheme : Boolean masking

Original version

```
Byte a = some_data();

Byte b = some_data();

Byte res = a ⊕ b;
```

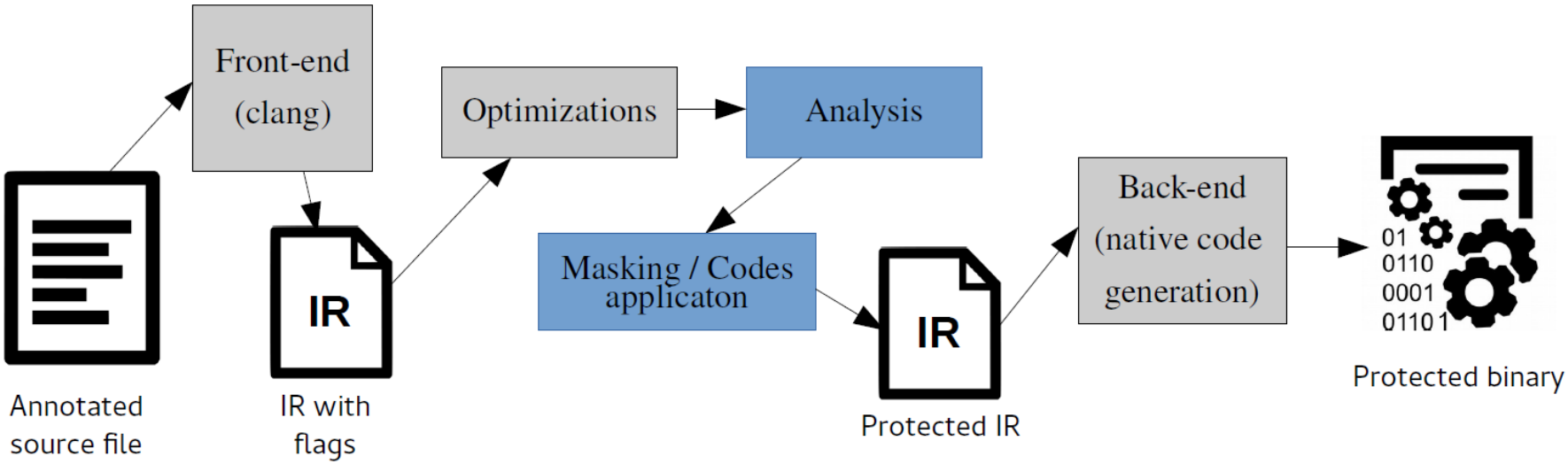
Masked version

```
Byte mask_a = rand();
Byte a = some_data() ⊕ mask_a;

Byte mask_b = rand();
Byte b = some_data() ⊕ mask_b;

Byte res = a ⊕ b;
```

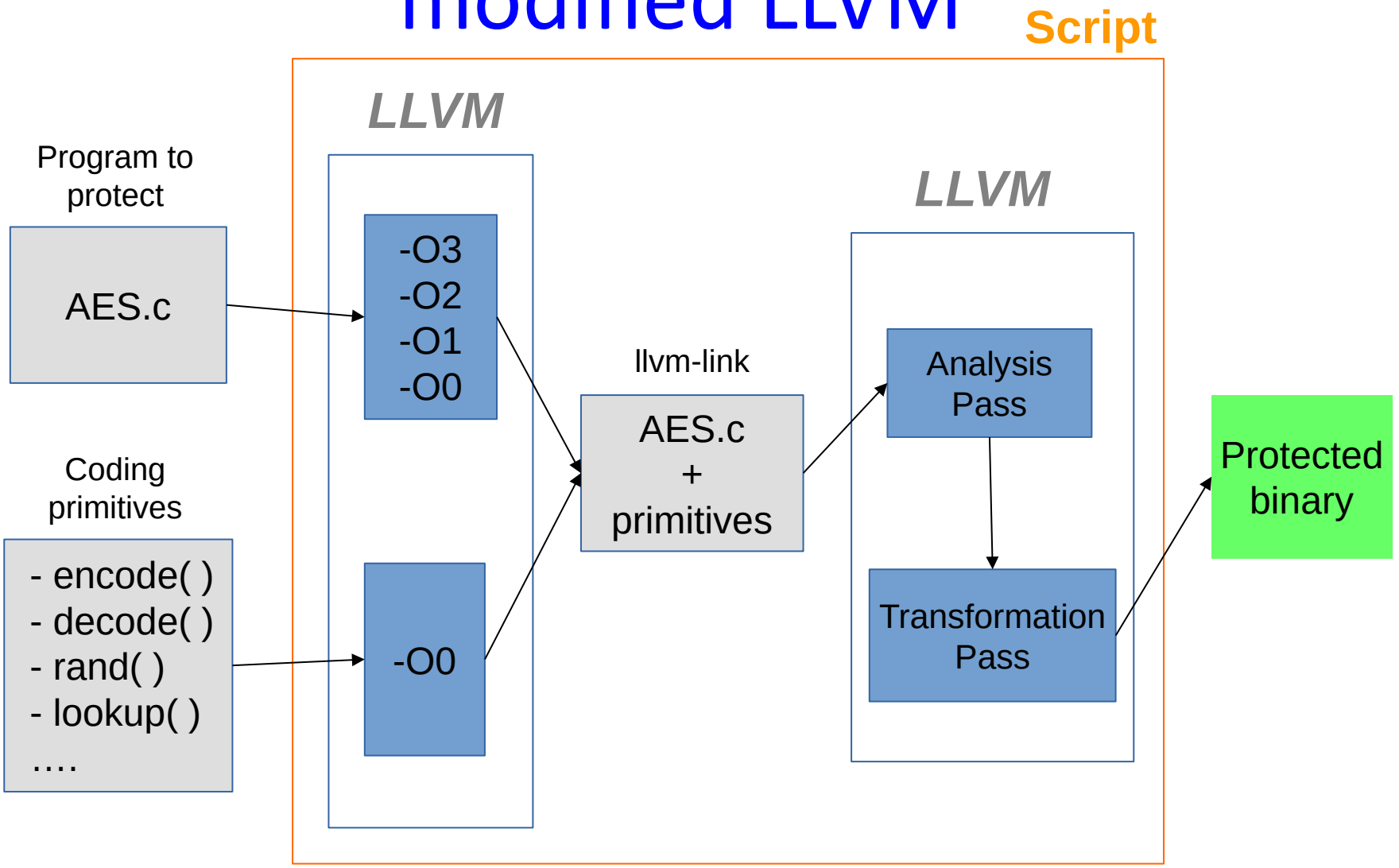
- Easy to understand for non-coding people
- Linear operations stay the same, non-linear need precomputations
- Can protect against passive side-channel attacks (e.g. DPA)
- The number of masks per variable N can be increased or decreased (resistant up to $N\text{-}1^{th}$ order attacks)

Code Implementation : modified LLVM

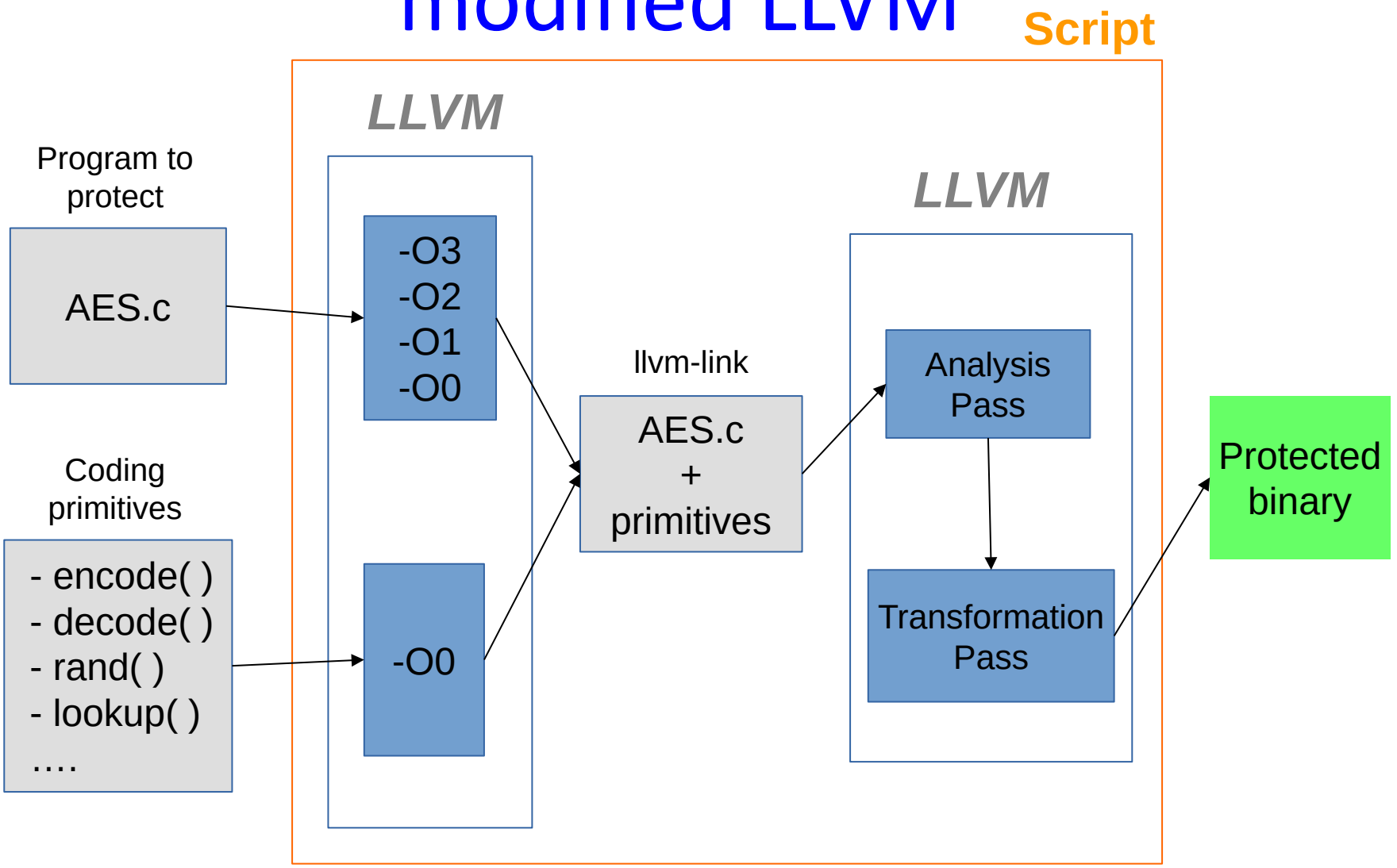
LLVM plugin overview



Code Implementation : modified LLVM



Code Implementation : modified LLVM



Publications

Revue

Sihem Mesnager, Chunming Tang and Yanfeng Qi, Complementary Dual Algebraic Geometry Codes. Submitted to IEEE Transactions on Information Theory.

Cem Guneri, Ferruh Ozbudak, Buket Ozkaya, Elif Sacikara, Zahra Sepasdar and Patrick Sole , *Structure and performance of generalized quasi-cyclic codes*, submitted to the journal “Finite Fields and Their Apllications”

Adel Alahmadi, Cem Guneri, Buket Ozkaya, Hatoon Shoaib and Patrick Sole , *On linear complementary-dual multinegacirculant codes*, submitted to the journal “Cryptography and Communications”

Claude CARLET and Sylvain GUILLEY , *Complementary Dual Codes for Counter-measures to Side-Channel Attacks*, in Adv. In Math. Of Comm, 2016, vol 10, n°1, p 131-150

International conferences

Weijia Wang, F.-X. Standaert, Yu Yu, Sihang Pu, Liuj Junrong, Zheng Guo, Dawu Gu *Inner Product Masking for Bitslice Ciphers and Security Order Amplification for Linear Leakages*, to appear in the proceedings of CARDIS 2016, Lecture Notes in Computer Science Cannes, France, November 2016, Springer

M.O. Choudary, R. Poussier, F.-X. Standaert, *Score-based vs. Probability-based Enumeration -- a Cautionary Note* --, in the proceedings of INDOCRYPT 2016, Lecture Notes in Computer Science, vol 10095, pp 137-152, Kolkata, India, December 2016, Springer

R. Poussier, F.-X. Standaert, V. Grosso, *Simple Key Enumeration (and Rank Estimation) using Histograms: an Integrated Approach*, in the proceedings of CHES 2016, Lecture Notes in Computer Science, vol 9813, pp 61-81, Santa Barbara, California, USA, August 2016, Springer

Sylvain Guilley, Annelie Heuser and Olivier Rioul, "Codes for side-channel attacks and protections," in Proc. 2nd Int. Conf. on Codes, Cryptology and Information Security, in honor of Claude Carlet, Rabat, Marocco, April 10-12, 2017. Lecture Notes in Computer Science, vol. 10194, Springer, 2017.
http://perso.telecom-paristech.fr/~rioul/publis/201704guilleyheuserrioul.pdf

Nicolas Bruneau, Claude Carlet, Sylvain Guilley, Annelie Heuser, Emmanuel Prouff and Olivier Rioul, "Stochastic Collision Attack," IEEE Transactions on Information Forensics & Security.
http://perso.telecom-paristech.fr/~guilley/16_IEEETIFS_collisions.pdf

Posters

SECODE presentation poster, at Rencontre inter UMRs-DGA 25/10/2016 Bruz, France (INRIA)

THANK YOU