Lyra2
Efficient Password Hashing with high security against Time-Memory Trade-Offs (TMTO)

Ewerton Rodrigues Andrade

eandrade@larc.usp.br

Escola Politécnica da Universidade de São Paulo – Poli/USP
São Paulo, SP – Brazil

Funding agencies:
CAPES and FDTE

Doctoral Consortium – 2nd ICISSP

19th February 2016

Agenda

1. Introduction
   - Motivation
   - Objectives
2. Lyra2
   - The Bootstrapping phase
   - The Setup phase
   - The Wandering phase
   - The Wrap-up phase
3. Comparison
   - Performance
   - Security
4. Conclusions
   - Stage of the research

Agenda

1. Introduction
   - Motivation
   - Objectives
2. Lyra2
   - The Bootstrapping phase
   - The Setup phase
   - The Wandering phase
   - The Wrap-up phase
3. Comparison
   - Performance
   - Security
4. Conclusions
   - Stage of the research

Motivation

User authentication is one of the most **vital elements** in modern computer security.

Motivation

User authentication is one of the most **vital elements** in modern computer security.

KNOW	HAVE	ARE
		
Passwords ID Questions Secret Images	Token (Smart) Card Phone	Face Iris Hand/Finger

Motivation *(Cont.)*

A study from 2007 shows that real users have passwords with a really **low entropy**, on average (approximate 40.5 bits [FH07])

It allows some "brute-force attacks":

- Dictionary
- Exhaustive search
- Pre-calculated tables (Rainbow tables, hash tables, ...)

Motivation *(Cont.)*

A study from 2007 shows that real users have passwords with a really **low entropy**, on average (approximate 40.5 bits [FH07])

It allows some "brute-force attacks":

- Dictionary
- Exhaustive search
- Pre-calculated tables (Rainbow tables, hash tables, ...)

How increase the cost of these attacks?

Using **Password Hashing Schemes** (PHS):

PBKDF2
bcrypt
scrypt
Lyra [our]

Objectives

Preserves the flexibility and efficiency of Lyra, including:

- **The ability to configure** the desired amount of memory, processing time and parallelism to be used by the algorithm *(flexibility)*
- The capacity of providing a **high memory usage** with a processing time similar to that obtained with scrypt *(efficiency)*

Objectives

Preserves the flexibility and efficiency of Lyra, including:

- **The ability to configure** the desired amount of memory, processing time and parallelism to be used by the algorithm *(flexibility)*
- The capacity of providing a **high memory usage** with a processing time similar to that obtained with scrypt *(efficiency)*

Improvements *(on security)*

When compared to its predecessor, Lyra2 add:

- A higher security level against attack venues involving time-memory trade-offs (**TMTO**)
- Includes tweaks for increasing the costs involved on the **construction of dedicated hardware** to attack the algorithm
- **Balance** resistance against **side-channel** attacks and attacks relying on cheaper (and, hence, slower) **storage devices**
- Allows legitimate users to benefit more effectively from the **parallelism** capabilities of their own platforms

Agenda

1. Introduction
   - Motivation
   - Objectives
2. Lyra2
   - The Bootstrapping phase
   - The Setup phase
   - The Wandering phase
   - The Wrap-up phase
3. Comparison
   - Performance
   - Security
4. Conclusions
   - Stage of the research

Overview *(Cryptographic Sponge)*

- We constructed Lyra2 upon **Cryptographic Sponge**

Why?

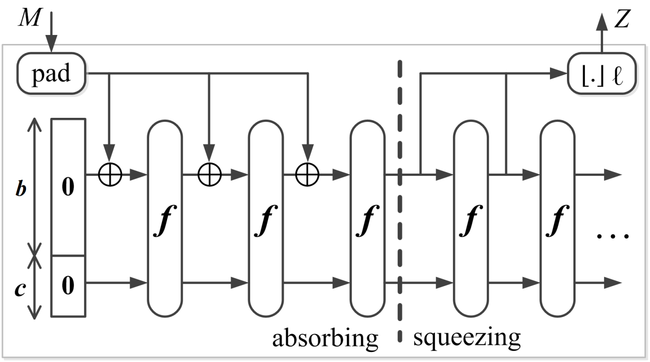
Elegant, Flexibly, **Secure**

Overview *(Cryptographic Sponge)*

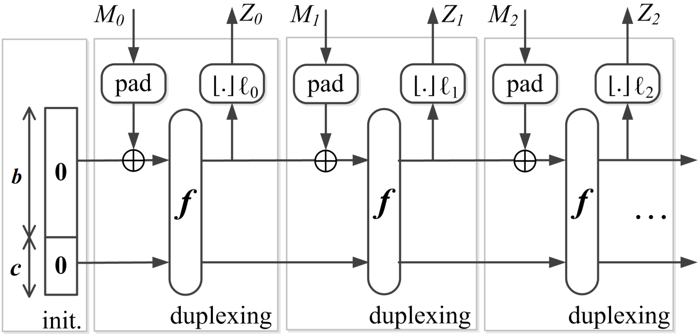
- We constructed Lyra2 upon **Cryptographic Sponge**

Why?

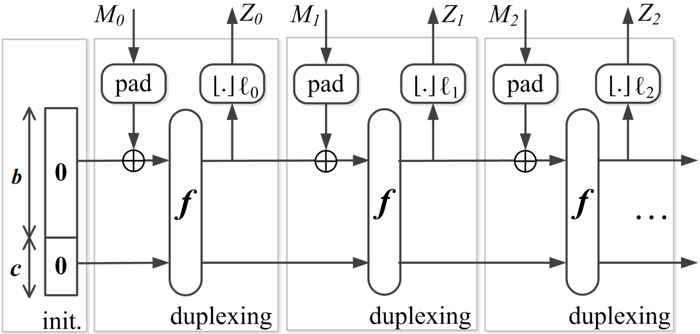
Elegant, Flexibly, **Secure**



Overview *(Cryptographic Sponge)*



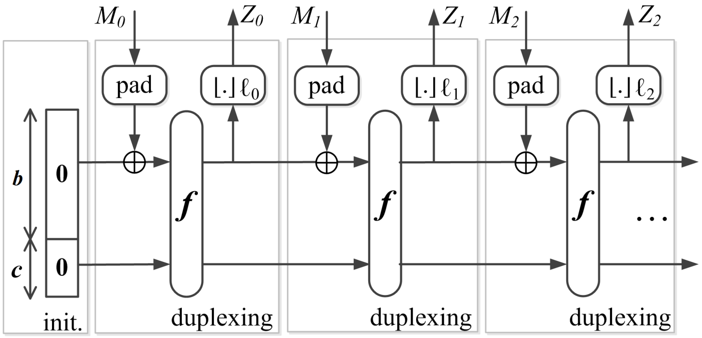
Overview *(Cryptographic Sponge)*



Instances

- Keccak (SHA-3), Quark, Photon, Spongent, Gluon ... [BDPA07]

Overview *(Cryptographic Sponge)*



Instances

- Keccak (SHA-3), Quark, Photon, Spongent, Gluon ... [BDPA07]

PHC special recognition

"for its elegant sponge-based design" [PHC15]

Overview

- Based on four phases
  - **Bootstrapping**: Init. the sponge's state and local variables
  - **Setup**: Initializes a memory matrix
  - **Wandering**: Iteratively overwrites of the memory matrix
  - **Wrap-up**: Output computation

The Bootstrapping phase

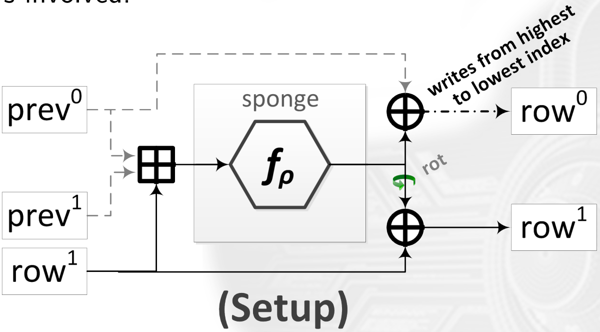
Initializes the sponge's state and local variables

- Absorb: *pwd*, *salt*, and *parameters*
- Initializes variables *(counters)*

The Setup phase

Initializes a memory matrix

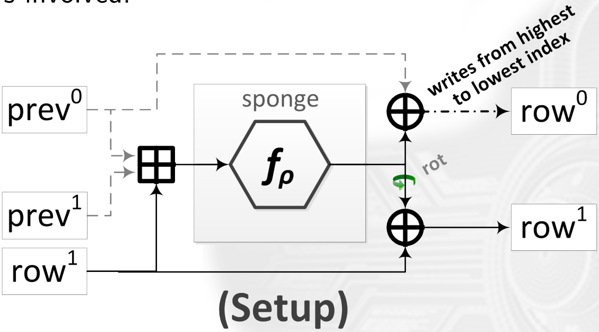
- Deterministically *(i.e., protected against side-channel attacks)*
- Rows involved:



The Setup phase

Initializes a memory matrix

- Deterministically *(i.e., protected against side-channel attacks)*
- Rows involved:

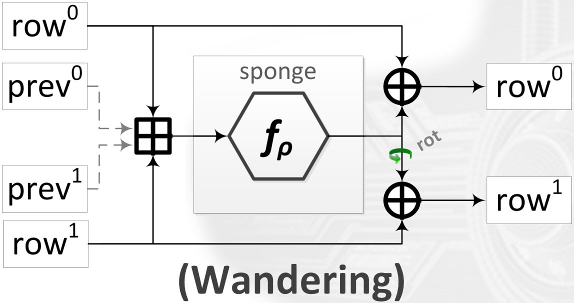


- Make **pipelining** harder, and increase the **latency in hardware**

The Wandering phase

Iteratively overwrites pseudorandom rows of the memory matrix

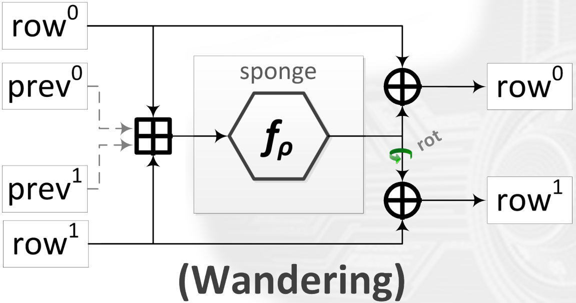
- Pseudorandomly *(increase TMTO)*
- Also the columns are picked pseudorandomly *(decrease performance: GPUs and platf. with small cache)*
- Rows involved:



The Wandering phase

Iteratively overwrites pseudorandom rows of the memory matrix

- Pseudorandomly *(increase TMTO)*
- Also the columns are picked pseudorandomly *(decrease performance: GPUs and platf. with small cache)*
- Rows involved:



- Prioritise **legitimate platforms**, and increase the **cost of ded. hardware**

The Wrap-up phase

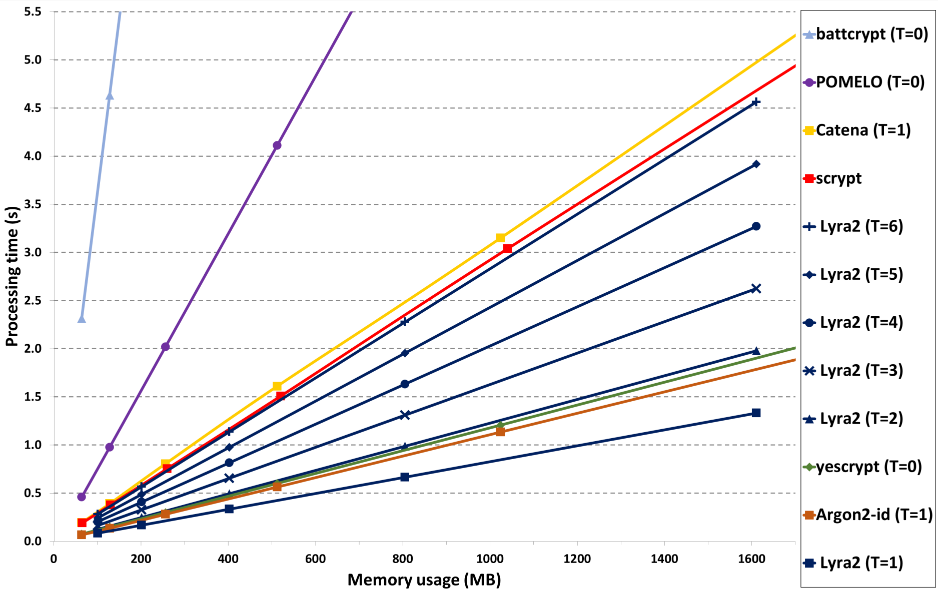
Output computation

- Provides *k*-long bitstring as output

Agenda

1. Introduction
   - Motivation
   - Objectives
2. Lyra2
   - The Bootstrapping phase
   - The Setup phase
   - The Wandering phase
   - The Wrap-up phase
3. Comparison
   - Performance
   - Security
4. Conclusions
   - Stage of the research

Performance



Slow-Memory and Cache-timing attacks

Slow-Memory

X

Cache-timing
(side-channel)

Slow-Memory and Cache-timing attacks

Slow-Memory

X

Cache-timing
(side-channel)

PHC special recognition

"alternative approach to side-channel resistance" [PHC15]

Low-Memory attack

- When the memory used by the attacker is **smaller than the half** amount of memory used during the legitimate process (i.e., $\frac{R}{2^{n+2}}$, where $n \geq 0$)
- The "dependence tree" grows significantly, resulting in the follow **complexity**:

$$\mathcal{O}(2^{2nT} R^{2+n/2}), \text{ for } n \gg 1$$

Propose with the **best TMTO** on PHC context!

Agenda

1 Introduction
- Motivation
- Objectives

2 Lyra2
- The Bootstrapping phase
- The Setup phase
- The Wandering phase
- The Wrap-up phase

3 Comparison
- Performance
- Security

4 Conclusions
- Stage of the research

Stage of the research

- In our doctoral work we present a new PHS that **maintaining the efficiency and flexibility** of its predecessor, and **increases its security** in terms of:
  - TMTO
  - Costs involved on the construction of dedicated hardware
  - Balance between side-channel ans slow memory attacks
  - Possibility to explore parallelism on legitimate platforms

Stage of the research

- In our doctoral work we present a new PHS that **maintaining the efficiency and flexibility** of its predecessor, and **increases its security** in terms of:
  - TMTO
  - Costs involved on the construction of dedicated hardware
  - Balance between side-channel ans slow memory attacks
  - Possibility to explore parallelism on legitimate platforms

Publications and other results

- PHC special recognition [PHC15]
- Vertcoin move from scrypt to Lyra2 [a4314, Day14]
- Sgminer add support to Lyra2 in its releases [Cry15]
- Publications:
  - Lyra was published at JCEN [AABS14]
  - Abstract of Lyra2 was presented at LatinCrypt'14 [AS14]
  - Lyra2 was published at IEEE trans. on Computers [ASBS16]

Thank you!

References I

[a4314] a432511. PoW Algorithm Upgrade: Lyra2 – Vertcoin. https://vertcoin.org/pow-algorithm-upgrade-lyra2/. Accessed: 2015-05-06., 2014.

[AABS14] L. C. Almeida, E. R. Andrade, P. S. L. M. Barreto e M. A. Simplicio Jr. Lyra: Password-Based Key Derivation with Tunable Memory and Processing Costs. Journal of Cryptographic Engineering, 4(2):75–89, 2014. See also http://eprint.iacr.org/2014/030.

[AS14] E. R. Andrade e M. A. Simplicio Jr. Lyra2: a password hashing schemes with tunable memory and processing costs. Third International Conference on Cryptology and Information Security in Latin America, LATINCRYPT'14. Florianópolis, Brazil.http://latincrypt2014.labsec.ufsc.br/. Accessed: 2015-05-06, 2014.

[ASBS16] E. R. Andrade, M. A. Simplicio Jr, P. S. L. M. Barreto e P. C. F. dos Santos. Lyra2: efficient password hashing with high security against time-memory trade-offs. IEEE Transactions on Computers, 2016. See also http://eprint.iacr.org/2015/136.

[BDPA07] G. Bertoni, J. Daemen, M. Peeters e G. Van Assche. Sponge functions. (ECRYPT Hash Function Workshop 2007), 2007. http://sponge.noekeon.org/SpongeFunctions.pdf. Accessed: 2015-06-09.

[Cry15] Crypto Mining. Updated Windows Binary of sgminer 5.1.1 With Fixed Lyra2Re Support – Crypto Mining Blog. http://cryptomining-blog.com/4535-updated-windows-binary-of-sgminer-5-1-1-with-fixed-lyra2re-support/. Accessed: 2015-05-06, 2015.

[Day14] Timothy Day. Vertcoin (VTC) plans algorithm change to Lyra2 – coinbrief. http://coinbrief.net/vertcoin-algorithm-change-lyra2/. Accessed: 2015-05-06, 2014.

[FH07] D. Florencio e C. Herley. A Large-scale Study of Web Password Habits. Em Proceedings of the 16th International Conference on World Wide Web, páginas 657–666, New York, NY, USA, 2007. ACM.

[PHC15] PHC. PHC status report. https://password-hashing.net/report1.html. Accessed: 2015-05-06, 2015.

[SO12] D. Song e J. Oberheide. Modern Two-Factor Authentication: Defending Against User-Targeted Attacks. Duo Security, 2012. https://speakerdeck.com/duosec/modern-two-factor-authentication-defending-against-user-targeted-attacks. Accessed: 2015-07-06.

Credits

- The picture used as background follows the license contained in http://www.icissp.org/ – © International Conference on Information Systems Security and Privacy.
- The image used in Motivation slide was taken from [SO12] and follows the © GitHub Inc. license.
- The image used in Motivation *(Cont.)* slide was adapted from the websites images: http://1aled.fotomaps.ru/ and http://www.harvestsolutions.net/, following their respective licenses.
- The images used in the "Slow-Memory and Cache-timing attacks" slide were get from the websites http://www.toshiba.com/, http://www.engadget.com/ and https://wiki.teamfortress.com/; and follows the licenses of their sites.
- Other images used throughout this presentation were made by the authors.