КРИПТОНИТ

# Memory-Hard функции: обзор подходов к построению и анализу

**Анастасия Чичаева**, Степан Давыдов

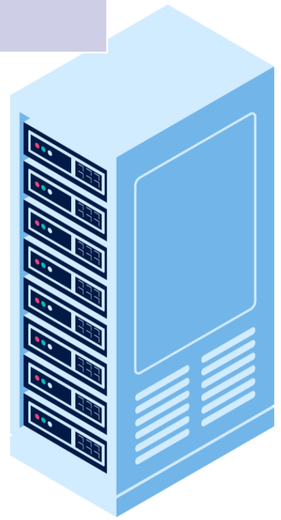
kryptonite.ru

# Схемы хэширования паролей

**Login1**
**password1**

**Login2**
**password2**

| База данных сервера | | |
|---|---|---|
| Login1 | Salt1 | Hash (Password1, Salt1) |
| Login2 | Salt2 | Hash (Password2, Salt2) |
| … | … | … |

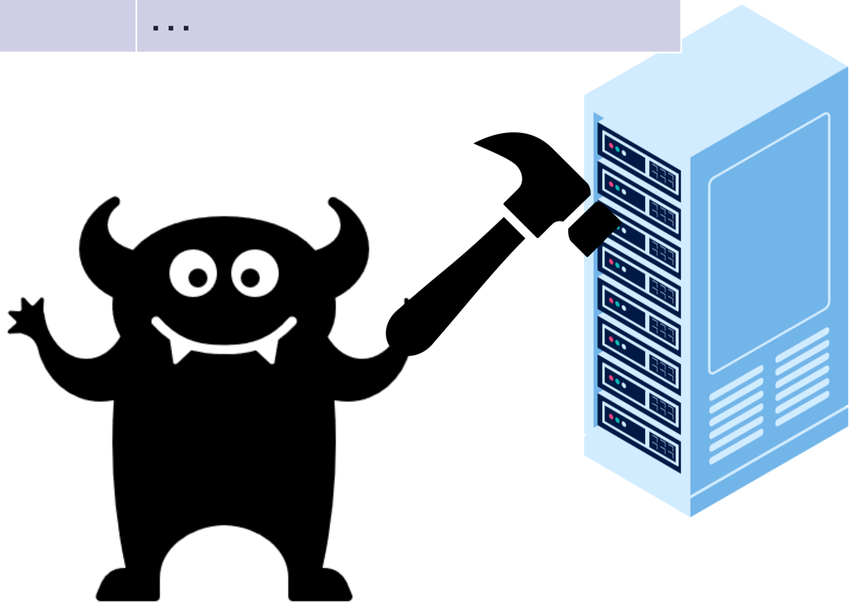


# Схемы хэширования паролей

**Login1**
**password1**

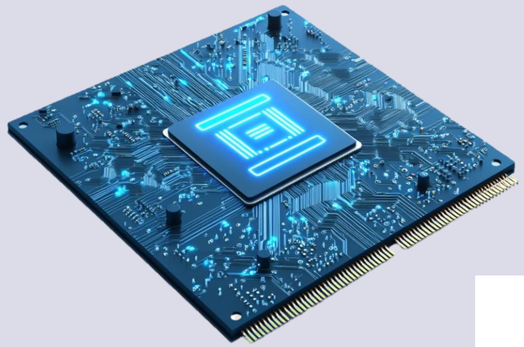
**Login2**
**password2**

| База данных сервера | | |
|---|---|---|
| Login1 | Salt1 | Hash (Password1, Salt1) |
| Login2 | Salt2 | Hash (Password2, Salt2) |
| … | … | … |



Brute-force атаки,
с использованием ASIC, FPGA и др.

# Переборные атаки



- Antminer S9 майнер Bitcoin: вычисляет SHA256 со скоростью до 13,6 триллионов хэшей в секунду, используя всего 1274 Ватт.

  *На CPU энергии требуется на **~6** порядков больше.*[1]

- Реализация PBKDF2 на FPGA в **~330** раз быстрее, чем на компьютерах. И потребляет в **~3** раза меньше энергии.[2]


[1] J. Blocki, L. Ren, and S. Zhou, Bandwidth-hard functions: Reductions and lower bounds, IACR Cryptology ePrint Archive 2018 (2018) 221

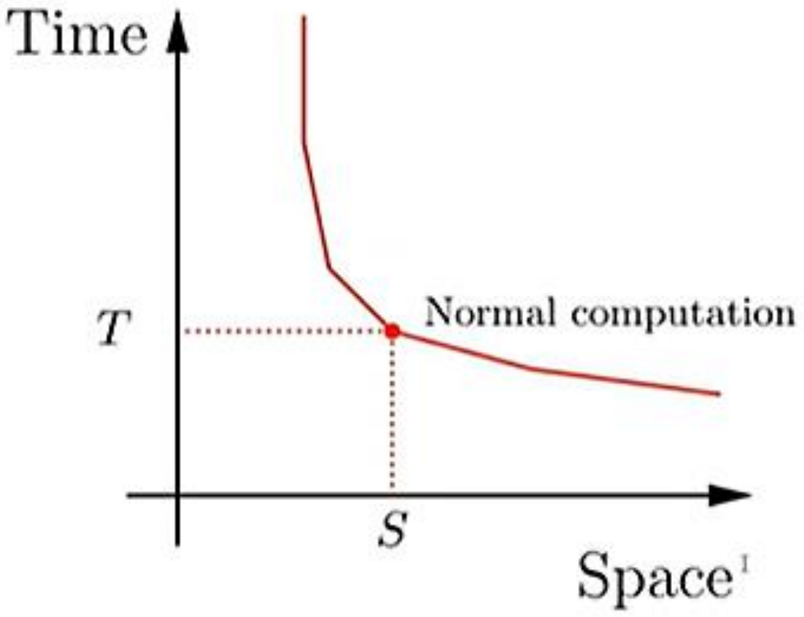
[2] Abbas, A.; Voss, R.; Wienbrandt, L.; Schimmler, M. An efficient implementation of PBKDF2 with RIPEMD-160 on multiple FPGAs. In Proceedings of the 20th IEEE International Conference on Parallel and Distributed Systems (ICPADS), Hsinchu, Taiwan, 16–19 December 2014; pp. 454–461.

# Memory-hard функции

**MHF** – это функции, для вычисления которых требуется значительный объём памяти, при этом незначительное уменьшение объёма памяти приводит к существенному возрастанию вычислительных ресурсов.

Неформальное определение:

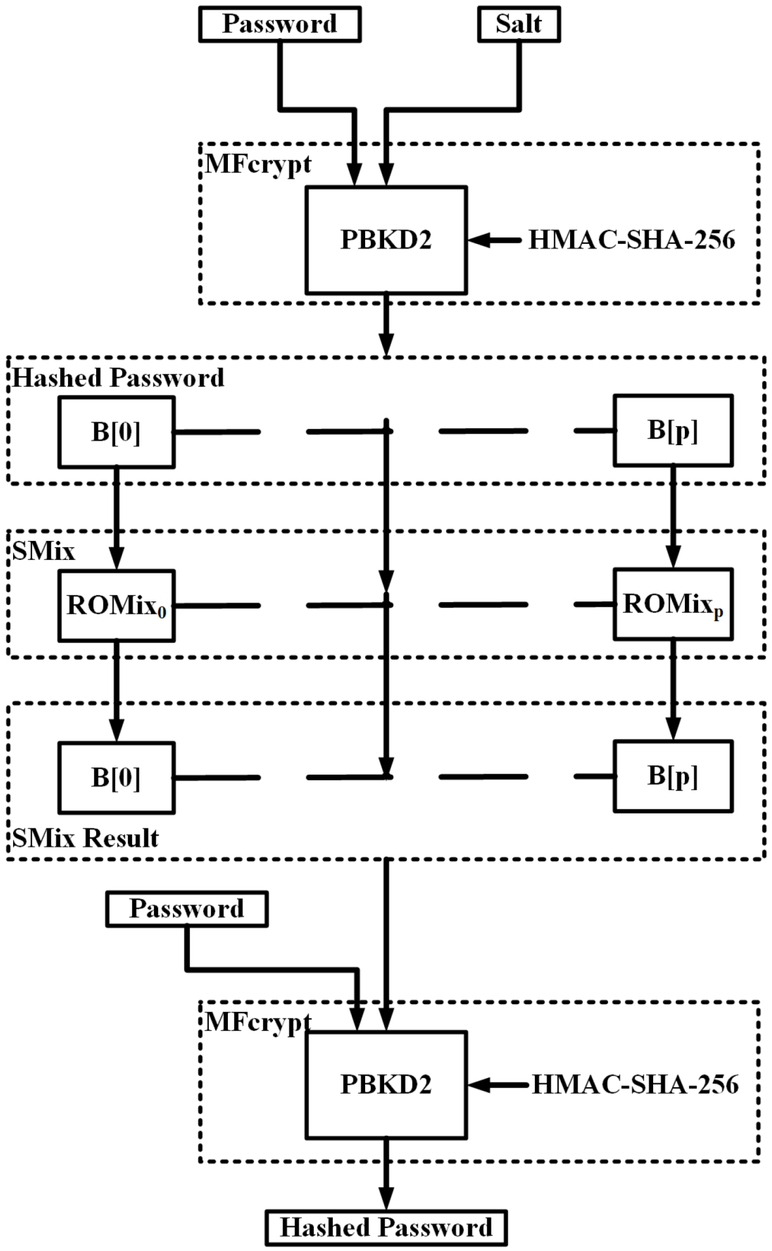
Невозможность значительно уменьшить величину $ST$ ($T' \gg T$, если $S' < S$), где $S$– площадь чипа, $T$– время работы.



# Memory-hard функции

## Scrypt

## Первая MHF – Scrypt[3]




[3] C. Percival, “Stronger key derivation via sequential memory-hard functions,” 2009.

# Password Hashing Competition

КРИПТОНИТ

- Проводился в 2013-2015
- 24 кандидата

Требования по безопасности:
- Криптографическая стойкость
- Невозможность значительного уменьшения потребление памяти
- Реализации на ASIC, FPGA и GPU не сильно повышают эффективность
- Устойчивость к атакам по побочным каналам

**Победитель: Argon2**
**Особое признание получили:**
- **Catena** за гибкую структуру и устойчивость к атакам по побочным каналам;
- **Lyra2** за интересную конструкцию на основе «губки» и альтернативный подход к защите от атак по побочным каналам;
- **Yescrypt** за разнообразие режимов работы, совместимость и простоту перехода от Scrypt;
- **Makwa** за конструкцию, основанную на задаче возведения в квадрат по модулю, и за уникальную функцию делегирования.

# Memory-Hard функции

КРИПТОНИТ

| Название | На чем основывается | Используемые алгоритмы | Используемая память |
|---|---|---|---|
| Scrypt | | Salsa20/8, PBKDF2, HMAC | 1ГБ |
| **Argon2 (победитель)** | | BLAKE2b, BlaMka | Argon2d:200МБ–4ГБ<br>Argon2i:1ГБ-6ГБ |
| Catena | Bit-Reversal Graph и Double-Butterfly Graph | BLAKE2b | BRG: 128МБ<br>DBG: 4МБ |
| battcrypt | | Blowfish, SHA-512 | 128КБ–128МБ |
| POMELO | Собственные конструкции | | 8КБ, 256 ГБ |
| Lyra2 | «губка» | BLAKE2b /BlaMka | 400МБ– 1ГБ |
| Makwa | возведения в квадрат | NIST HMAC_DRBG SHA-256 | 335 КБ |
| Pufferfish | Bcrypt | SHA-512, измененный Blowfish | 4КБ– 16КБ |
| Yescrypt | scrypt | SHA-256, Salsa20/8Core/ pwxform | ~1-3ГБ |
| Balloon | сэндвич-граф | Blake2b | 1МБ- 32МБ |

[4] *Hatzivasilis G.* Password-hashing status // Cryptography. — 2017. — Т. 1, №2. —С. 10

# Конструкции MHF

КРИПТОНИТ

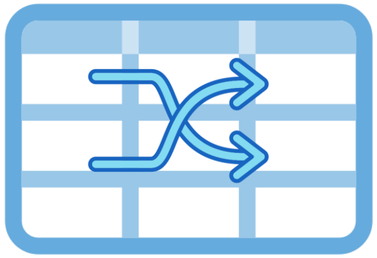
## Этапы вычисления MHF

1. Извлечение энтропии и начальное заполнение блоков памяти.
2. Итеративная работа с памятью.
3. Формирование выходного значения из блоков памяти.

PBKDF2, HMAC, SHA256, Blake2b, «губка» и др.

# Конструкции MHF

## Работа с памятью



Происходит итеративное «перемешивание» блоков памяти

## dMHF (data dependent)

Функции с доступом к памяти, зависящим от данных.

- Более непредсказуемые.
- Подвержены атакам по побочным каналам.
- Лучше подходят для криптовалют.

## iMHF (data independent)

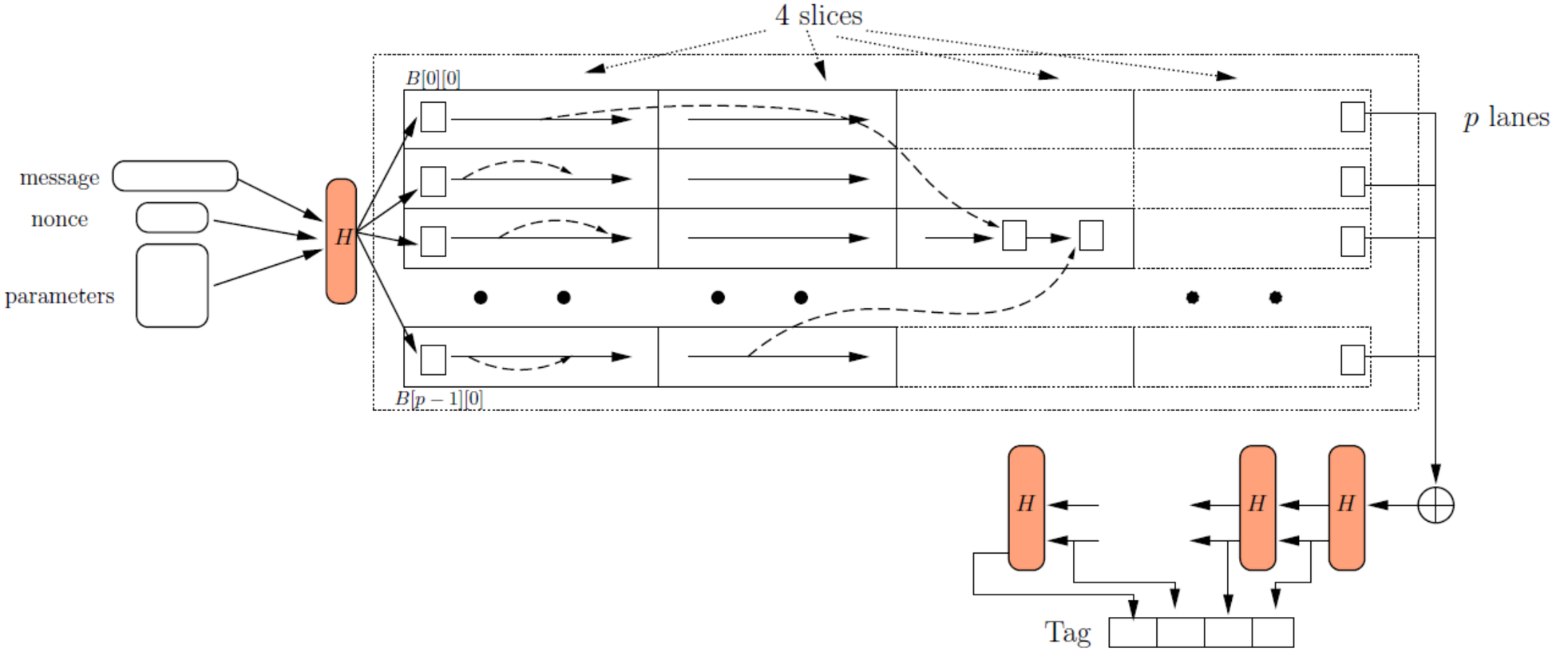
Функции с доступом к памяти, независящим от данных.

- Легче анализировать.
- Лучше подходят для хэширования паролей.
- Требуется больше проходов по памяти.

# Работа с памятью Argon2

$$B^t[i][0] = G(B^{t-1}[i][q-1], B[i'][j']) \oplus B^{t-1}[i][0],$$
$$B^t[i][j] = G(B^t[i][j-1], B[i'][j']) \oplus B^{t-1}[i][j].$$

$(i', j') \leftarrow \phi(\cdot)$ : функция индексации



# Применение MHF на практике

КРИПТОНИТ

- Scrypt применяется в криптовалюте Litecoin.
- Argon2 поддерживается для хэширования паролей в Ubuntu (20.04 и выше), NetBSD, NiceOS и др., а также в каталоге OpenLDAP.

# Методы анализа MHF

# Формализация свойства memory-hard

КРИПТОНИТ

***Определение 1.*** Алгоритм называется memory-hard в модели Random Access Machine (RAM), если для его вычисления используется $S(n)$ ячеек (объем памяти) и $T(n)$ операций, где $S(n) \in \Omega(T\,(n)^{1-\epsilon})$.

***Определение 2.*** Последовательная memory-hard функция – это функция такая, что:

- она может быть вычислена с помощью memory-hard алгоритма в модели RAM;
- она не может быть вычислена в модели Parallel Random Access Machine (PRAM) с $S^*(n)$ процессорами и $S^*(n)$ объемом памяти за время $T^*(n)$, где $S^*(n)T^*(n) = \mathcal{O}(T\,(n)^{2-x})$, $x > 0$.

[3] C. Percival, “Stronger key derivation via sequential memory-hard functions,” 2009.

# Формализация свойства memory-hard

КРИПТОНИТ

***Определение 1.*** Алгоритм называется memory-hard в модели Random Access Machine (RAM), если для его вычисления используется $S(n)$ ячеек (объем памяти) и $T(n)$ операций, где $S(n) \in \Omega(T\ (n)^{1-\epsilon})$.

***Определение 2.*** Последовательная memory-hard функция – это функция такая, что:

- она может быть вычислена с помощью memory-hard алгоритма в модели RAM;
- она не может быть вычислена в модели Parallel Random Access Machine (PRAM) с $S^*(n)$ процессорами и $S^*(n)$ объемом памяти за время $T^*(n)$, где $S^*(n)T^*(n) = \mathcal{O}(T\ (n)^{2-x})$, $x > 0$.

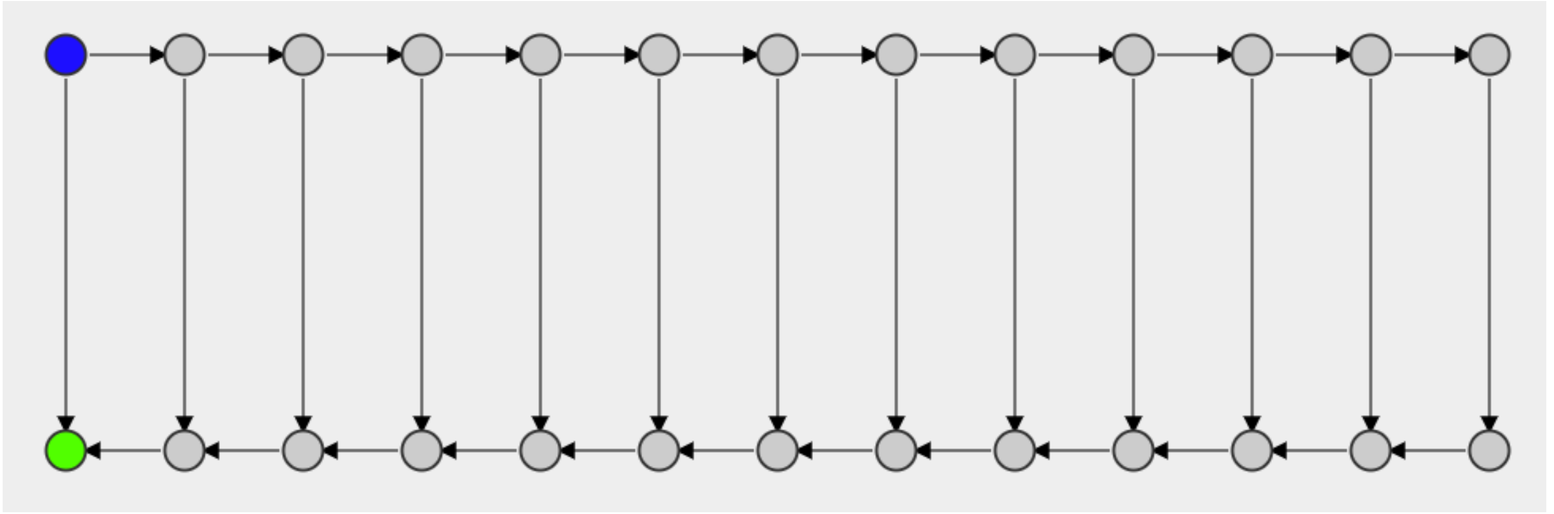
Не релевантная

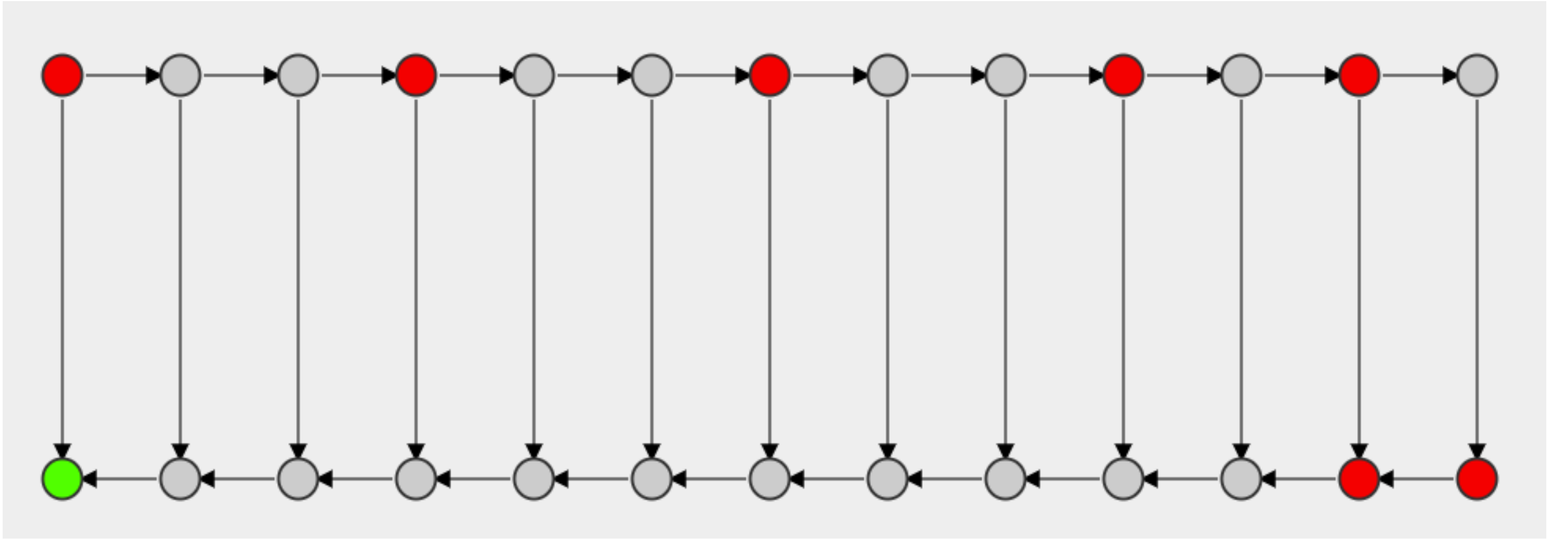
[3] C. Percival, “Stronger key derivation via sequential memory-hard functions,” 2009.

# Теория графов для анализа MHF

КРИПТОНИТ

## Black Pebbling Game

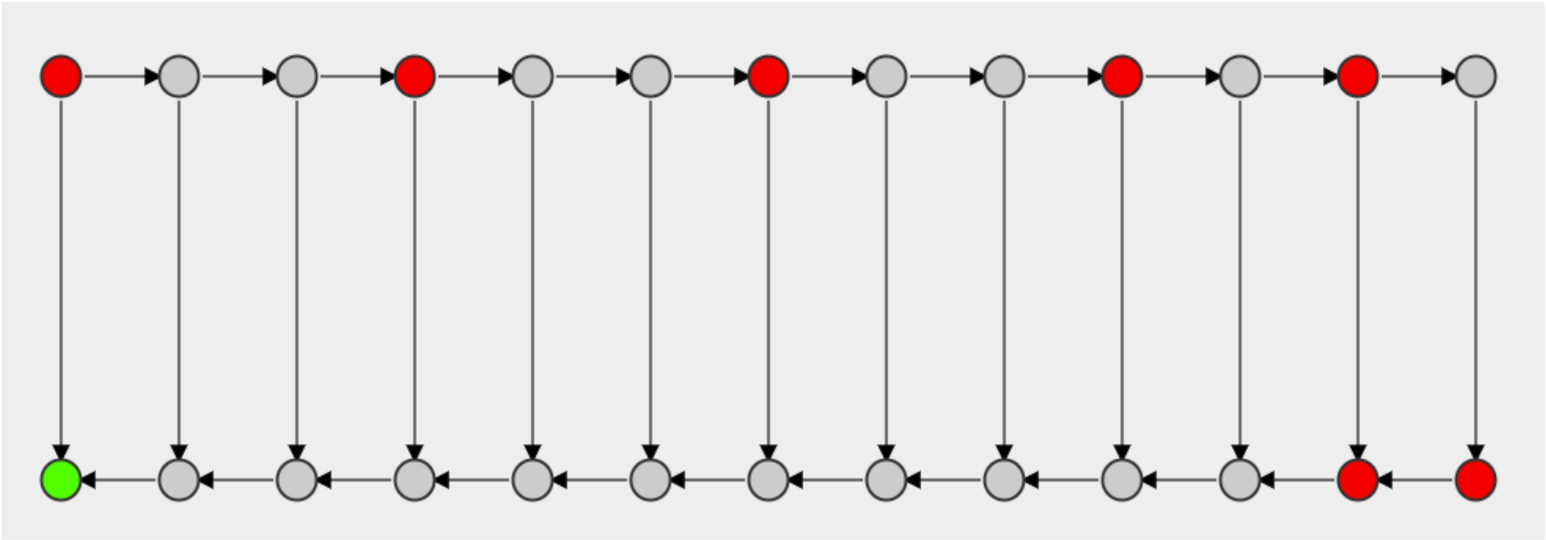




# Теория графов для анализа MHF

КРИПТОНИТ

## Black Pebbling Game



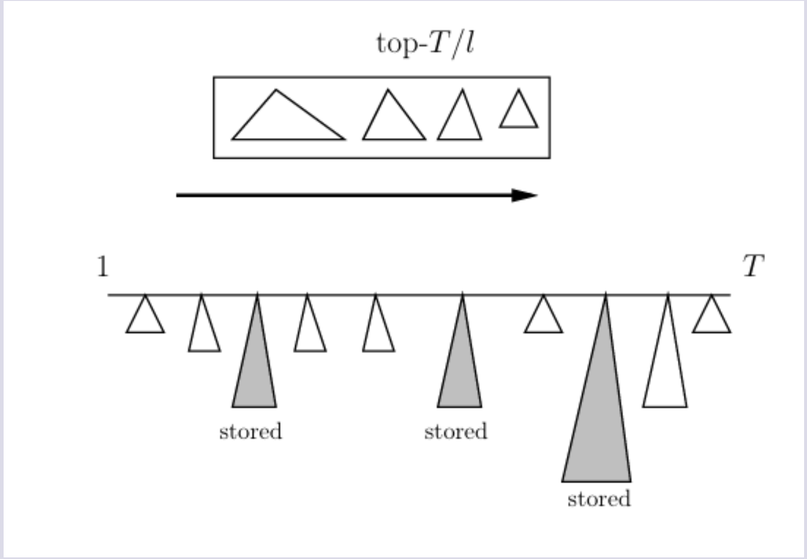
Стратегия $\mathrm{P} = (P_0, P_1, \ldots, P_t)$, где $P_i \subseteq \mathbb{V}$

Метрики:

- ST-сложность: $st(P) = t \cdot \max_{i \in [t]} |P_i|$ ;
- Накопленная сложность (cumulative complexity): $cc(P) = \sum_{i=0}^{t} |P_i|$ ;
- Sustained Space Complexity (SS-сложность): Для стратеги $P$ $m$-SS-сложность равна $t'$, если $|\{i : |P_i| \geq m\}| \geq t'$ (существует минимум $t'$ шагов, использующих объем памяти больший $m$).

# Атаки «Компромисса» на iMHF

## Метод ранжирования




Стратегия атаки.

1. Выбирается число $q$.
2. В памяти сохраняют блоки $B[kq]$ для всех $k$.
3. Для каждого блока вычисляется и сохраняется сложность доступа к нему.
4. Дополнительно в память сохраняют $T/q$ блоков с самой большой сложностью доступа.

[5] *BiryukovA.*, *Khovratovich D.*Tradeoff cryptanalysis of memory-hard functions .

# Атаки «Компромисса» на iMHF

КРИПТОНИТ

## Анализ графа функции

***Определение 3.*** Ориентированный ациклический граф $\mathbb{G} = (\mathbb{V}, \mathbb{E})$ называется $(e, d)$ - сократимым, если существует подмножество вершин $S \subseteq \mathbb{V}$, такое что $|S| \leqslant e$ и $depth(\mathbb{G} - S) \leqslant d$.
Если граф $\mathbb{G}$ не является $(e, d)$-сократимым, говорят что он обладает свойством $(e, d)$-надежности глубины (Depth Robustness).

***Идея атаки***: Если граф $(e, d)$ –сократимый, то можно хранить вершины из небольшого множества $S$ ($|S| \leq e$), а остальные вычислять при необходимости.

Атака состоит из двух фаз.

### «Легкая»

- Удаление лишних вершин
- Выполнение вычислений

### «Раздуваемая»

- Восстановление удаленных вершин

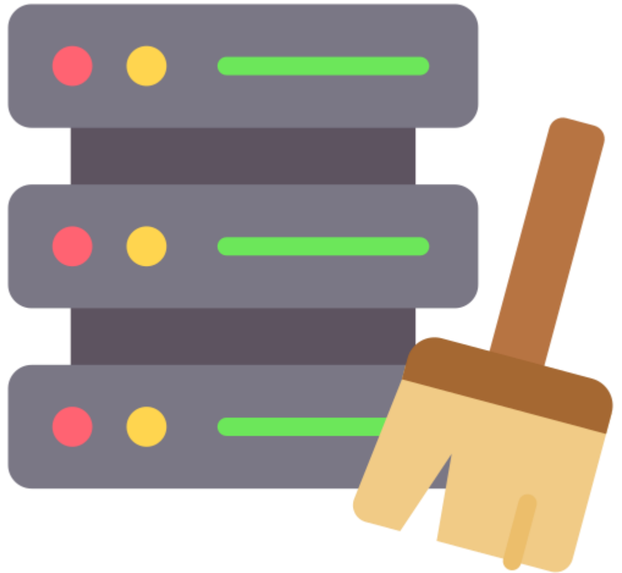
[6] Alwen J., Blocki J. Efficiently computing data-independent memory-hard functions // Annual International Cryptology Conference. — Springer. 2016. — С. 241—271.

# Атаки по побочным каналам

КРИПТОНИТ

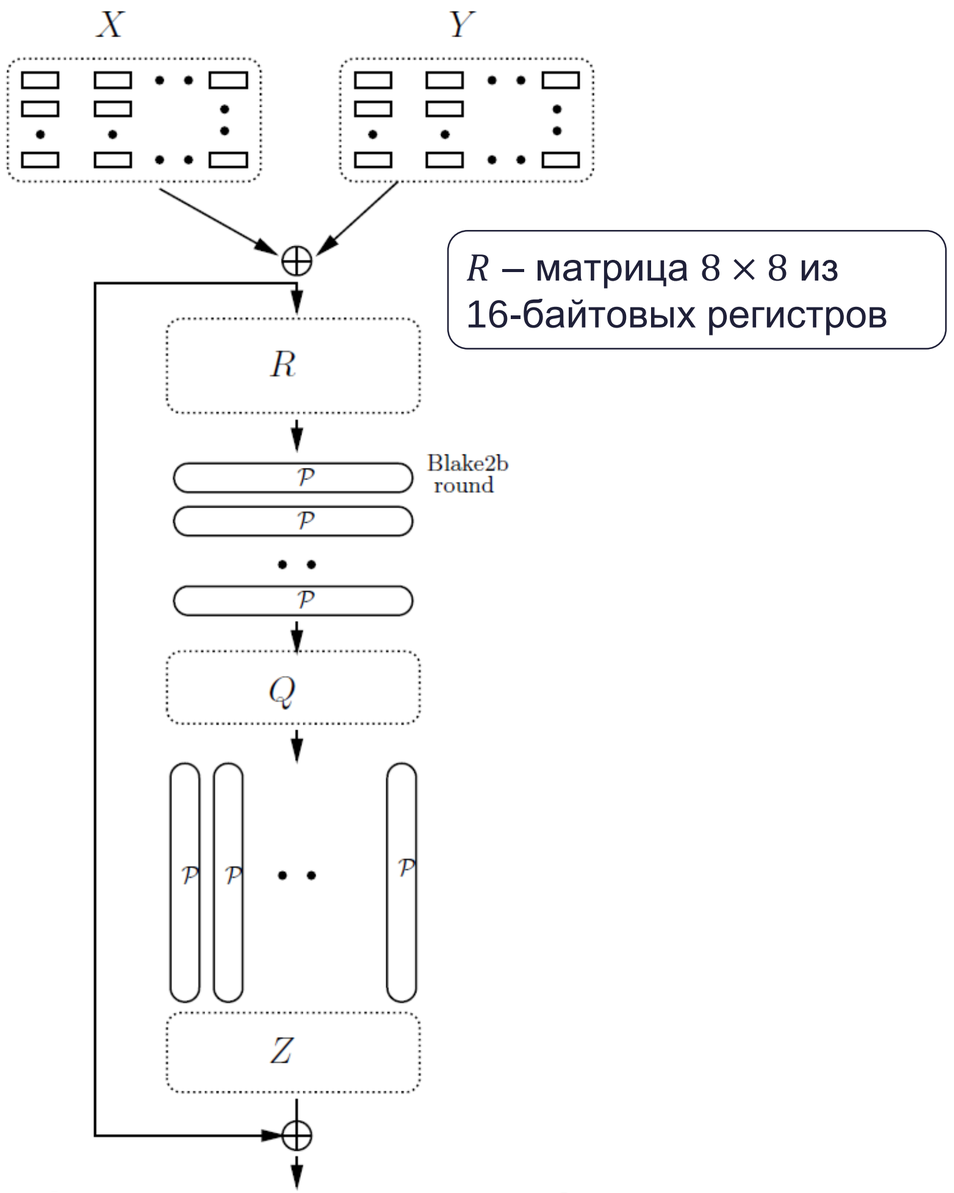
## Атаки «сборщика мусора»

## Атаки на основе доступа к кэш-памяти



# Перспективы отечественной MHF

- На начальном и финальном этапах можно использовать стандартизированные алгоритмы (PBKDF2 , HMAC,  Стрибог).
- Конструирование этапа работы с памятью требует дальнейших исследований.




**Функция сжатия Argon2**

КРИПТОНИТ

# Спасибо за внимание!

**Авторы доклада:**

Чичаева Анастасия

Специалист-исследователь,

Лаборатория криптографии

a.chichaeva@kryptonite.ru

Давыдов Степан

Старший специалист-исследователь,

Лаборатория криптографии

s.davydov@kryptonite.ru