

PROJECT

ЗАЩИЩЕННАЯ БАЗА ДАННЫХ

JOIN GROUPS & FOREIGN KEYS

DATE

SUMMER'2014

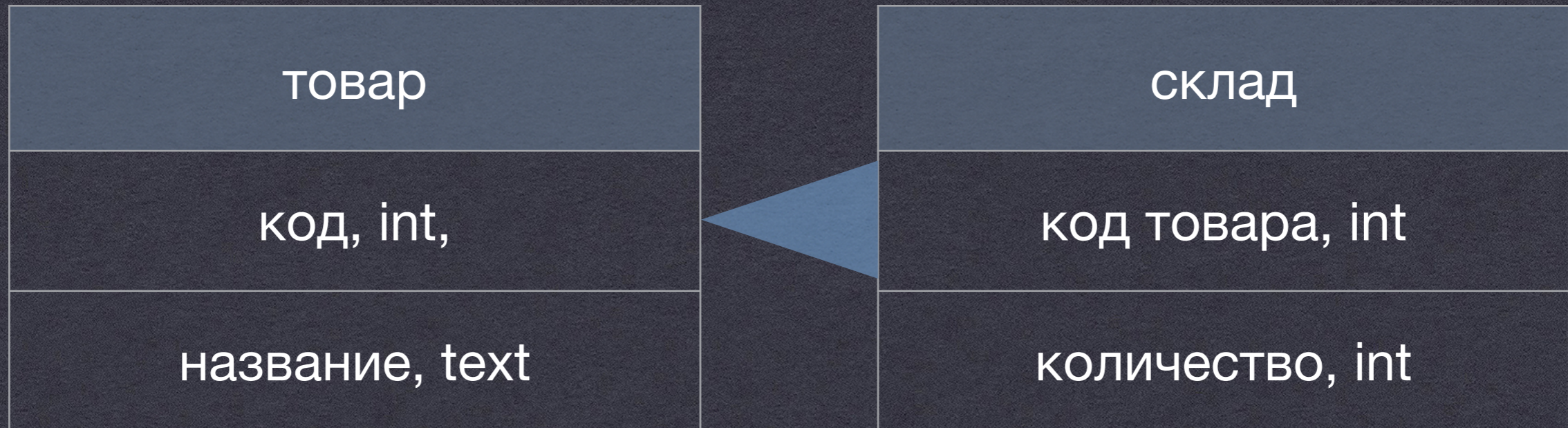
CLIENT

ШАТИЛОВ КИРИЛЛ

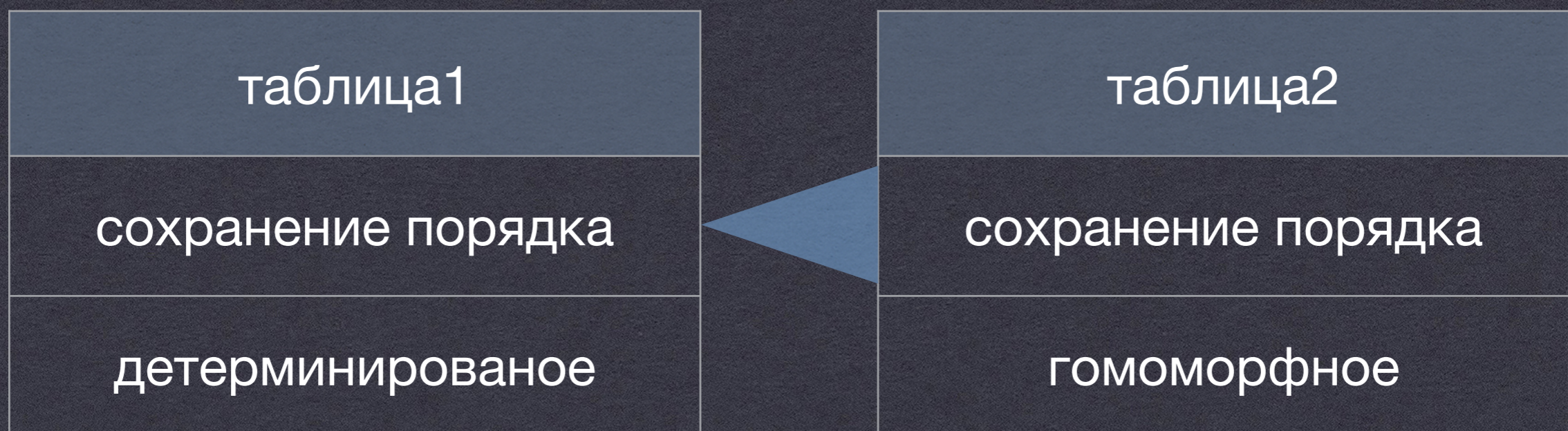
ТРЕБОВАНИЯ

1. Одно шифрование
2. Общий ключ
3. Детерминированность шифрования

СХЕМА ДАННЫХ



ШИФРОВАНИЕ



ЗАПРОСЫ CREATE

```
CREATE TABLE products
```

```
(  
  prod_id INT encrypted_oper join_group JG_1,  
  prod_descr TEXT encrypted_mgalois  
)
```

```
CREATE TABLE stock
```

```
(  
  prod_id INT encrypted_oper join_group JG_1,  
  quantity INT encrypted_homomorphic  
)
```

ЗАПРОСЫ CREATE

```
CREATE TABLE table1
```

```
(
```

```
    datarow1823467 BLOB,
```

```
    datarow4421377 BLOB
```

```
)
```

```
CREATE TABLE table2
```

```
(
```

```
    datarow4558725 BLOB,
```

```
    datarow1823454 INT,
```

```
    datarow1823454 INT,
```

```
    datarow1823454 INT,
```

```
    datarow1823454 INT
```

```
)
```

ЧТО ПРОИЗОШЛО

Хранилище крипто метаданных:

исходное имя	ключ	...	идентификатор JOIN_GROUP
prod_id	XXXYYY		JG_1
prod_id	XXXYYY		JG_1

ЧТО ПРОИЗОШЛО

обработка CREATE:

JOIN_GROUP

JOIN_GROUP
существует

запрос в Storage

JOIN_GROUP
не существует

создать ссылку
на ключ

запись в Storage

создать ключ

ДАЛЬНЕЙШАЯ РАБОТА

prod_id	prod_descr
1	'ZZZ'
2	'YYY'
3	'UUU'

prod_id	prod_quantity
1	100
2	200

SELECT

```
SELECT * FROM stock  
JOIN products  
ON products.id = stock.pro_id
```

prod_id	prod_descr	quantity
1	'ZZZ'	100
2	'YYY'	200

FOREIGN KEY

```
CREATE TABLE stock
```

```
(
```

```
  prod_id INT encrypted_oper,
```

```
  quantity INT encrypted_homomorphic
```

```
  FOREIGN KEY (prod_id) REFERENCES
```

```
  products(prod_id)
```

```
)
```

```
FOREIGN KEY ~ JOIN_GROUP
```

ИТОГО

Хранилище крипто
метаданных

- **изменение внутренних структур**
- **изменение интерфейса**

Грамматика CREATE

- **добавление новых правил**

Обработка CREATE

- **добавление новых функциональных элементов**

ВОПРОСЫ