Quark를 적용한 단건 배달 관리 시스템

https://youtu.be/dyhI3iLJokc

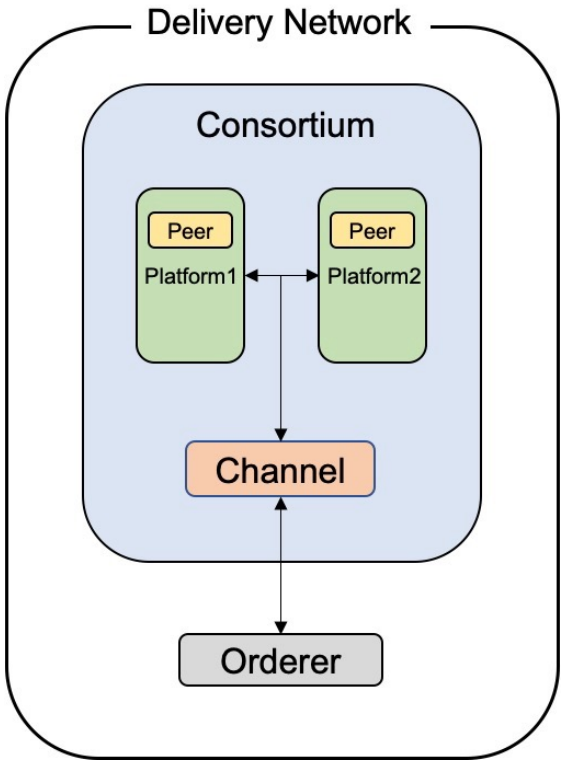
기존 시스템

Quark

Quark를 적용한 시스템

기존 시스템

- **기본 아이디어**
  - 단건 배달을 여러 플랫폼(배민1, 쿠팡이츠)에서 묶어서 배달하는 다중 배달 문제
  - 블록체인 시스템을 통해 다중 배달을 하지 못하도록 방지
    - 휴대 기기 고유 번호인 IMEI 사용 (15자리)
    - 블록체인 특성상 개인정보 유출 문제 발생

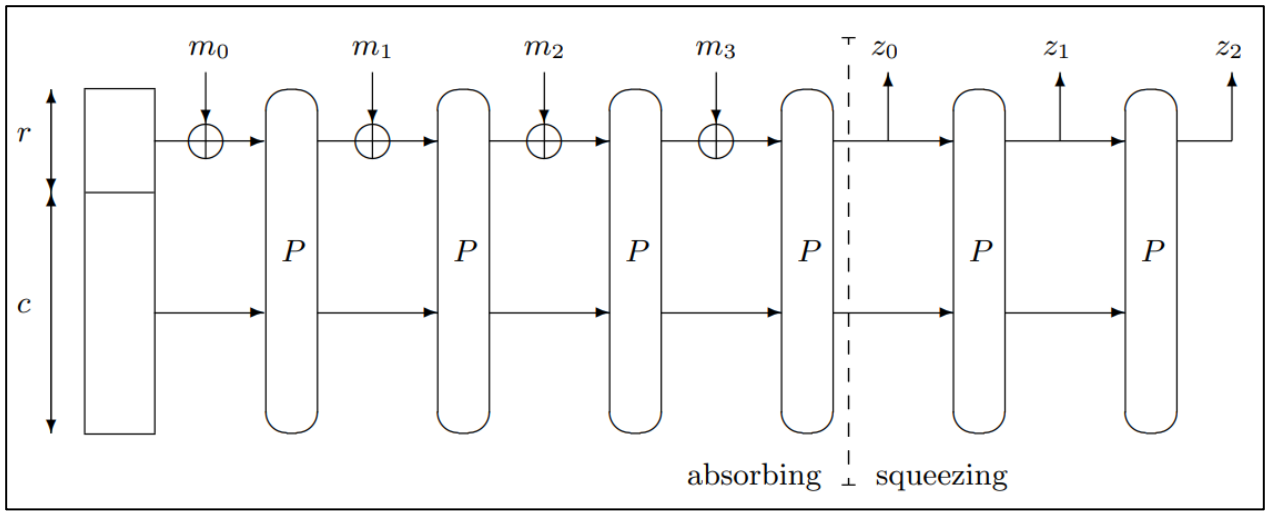


Quark

- 모바일 환경에 적합한 경량 해시함수
- u-Quark, d-Quark, s-Quark, c-Quark로 분류

경량화 ⟷ 보안

- Sponge 구조
  - Absorbing단계와 Squeezing단계로 구성



Quark

- u-quark
- | r = 8bits | c = 128bits |
- | message block = 8bits |
- | output: 136bits |

- 보안 강도: 64bit
- GE(gate equivalents): 1379개
- Keccak(2520GE)

```
while (databytelen > 0) {

    /* get next byte */

    console.log("data:", data.toString(16));


    var sliced_data = Math.floor(data / ((2 ** 8) ** (databytelen - 1)));
    console.log("sliced_data:", sliced_data.toString(16));
    var u: any = sliced_data & 0xff;

    console.log("get byte: " + u.toString(16) + " // at pos: " + state.pos);
    console.log("databytelen:", databytelen);


    /* xor state with each bit */
    for (i = 8 * state.pos; i < 8 * state.pos + 8; ++i) {

        console.log("(u >> (i % 8)) & 1:", (u >>> (i % 8)) & 1)
        state.x[(8 * (WIDTH - RATE)) + i] ^= (u >>> (i % 8)) & 1;
    }

    databytelen -= 1;
    state.pos += 1;

    if (state.pos == RATE) {
        U_permute(state.x);
        state.pos = 0;
    }

}
```

Absorbing 과정

Quark

- u-quark
- | r = 8bits | c = 128bits |
- | message block = 8bits |
- | output: 136bits |

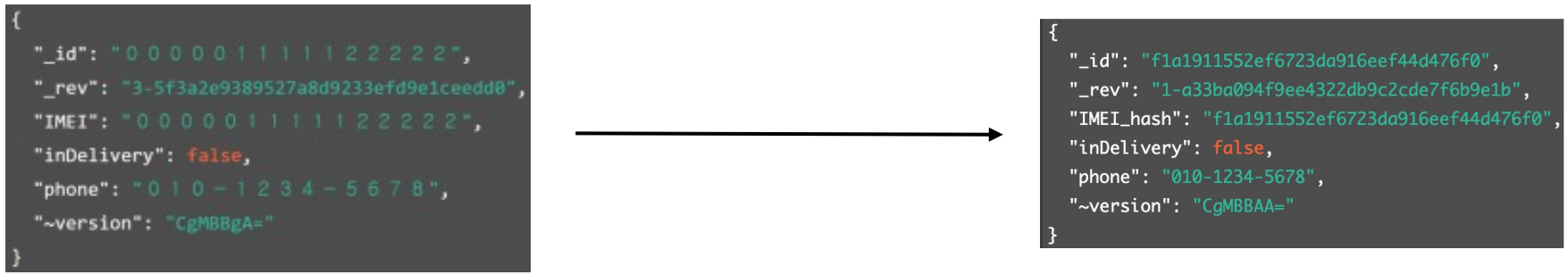
- 보안 강도: 64bit
- GE(gate equivalents): 1379개
- Keccak(2520GE)

```
while (outbytes < DIGEST) {

    /* extract one byte */
    for (i = 0; i < 8; ++i) {
        u = state.x[8 * (WIDTH - RATE) + i + 8 * (outbytes % RATE)] & 1;
        out[outbytes] ^= (u << (7 - i));
    }

    console.log("extracted byte %d (%d)\n", out[outbytes].toString(16), outbytes);

    outbytes += 1;
    console.log("outbytes:", outbytes);
    if (outbytes == DIGEST)
        break;

    u_showstate(state.x);

    /* if RATE bytes extracted, permute again */
    if (!(outbytes % RATE)) {
        U_permute(state.x);
    }
}
```

Squeezing 과정

Quark를 적용한 시스템

- 결과



Q & A