Privacy Analysis of Whisk

Dmitry Khovratovich

January 11, 2022

1 Notation

- N is the number of trackers;
- K is the stir size;
- s is the number of rounds (with N/K stirs in each).

2 Feistel stir selection rule

We represent trackers as a $K \times K$ matrix M. Then define $F(x, y)$ as

$$F(x, y) = (y, x + y^3 \bmod K).$$

Finally, we define that i-th proposer of r-th round selects for stirring the i-th row of matrix $F^k(M)$.

We say that the tracker selection rule is *uniform* if all trackers of a single stir will be processed by distinct proposers in the next and in the after-next rounds.

Proposition 1. *The Feistel rule is uniform for $K = 128$.*

Proof. The proof is easy: for $y_1 \neq y_2$ we have

$$\begin{aligned} F(x, y_1) &= (y_1, x + y_1^3); & F^2(x, y_1) &= (x + y_1^3, y_1 + (x + y_1^3)^3); \\ F(x, y_2) &= (y_2, x + y_2^3); & F^2(x, y_2) &= (x + y_2^3, y_2 + (x + y_2^3)^3) \end{aligned}$$

where $x + y_1^3 \neq x + y_2^3$ as $y \mapsto y^3$ is bijective modulo 128. $\square$

The uniformity of the Feistel rule implies that 1- and 0-touchers of each round are uniformly spreaded to stirs of the next rounds, which can be formulated as follows.

Proposition 2. *Let $\mathcal{S}$ be any subset of stirs with a uniform rule such that in round r fraction α_r of stirs are in $\mathcal{S}$. Then the fraction of 1-touchers after round k is*

$$F_1(k) = \prod_{r \leq k} (1 - \alpha_r).$$

3 Privacy analysis

Here we prove bounds on the censorship costs. First we outline the adversarial strategy that we presume optimal:

- Adversary knows the stirs of fraction β proposers.

- There are additionally γ proposers that go offline every day, and they are known to the adversary.
- During the day, the adversary kills all 0-touchers as they are the cheapest.
- He orders the remaining $(1-\beta-\gamma)$ trackers by the anonymity set size.
- Adversary shuts 1-touchers starting from the least anonymous ones.

Now we utilize the property of the Feistel rule.

Proposition 3. *Let fraction $\alpha > 0.01$ of proposers be honest and alive. Then the total number of 0-touchers before final filtering is at most*

$$W(\alpha) = \frac{-1.25N\ln\alpha}{K}$$

Proof. Let us find how many trackers can evade the fraction α of stirs and thus become 0-touchers.

For some W bigger than K let us select randomly W trackers and a single stir. The probability for all the trackers to miss the stir is $p = (1-\frac{K}{N})^W \approx e^{-\frac{WK}{N}}$. Consider stirs $\mathcal{S}_j = \{S[1,j], S[2,j], \ldots, S[s,j]\}$ i.e. those that are j-th in their round. The number ν_j of stirs in S not touching any of those W trackers is a random variable, which is the sum of s independent Bernoulli variables with mean p, and so has Binomial distribution with parameters (s,p). Note that random variables ν_j have negative covariance, so the total number ν of stirs not touching any of W trackers can be upper bounded by the variable with distribution $Bin(N/K \cdot s = N/2, p)$. The latter distribution can be approximated by normal one with parameters $(\mu = Np/2, \sigma^2 = Np(1-p)/2)$. With probability e^{-80} we have that the value of ν is at most

$$X(W) = \mu + 12\sigma = Ne^{-\frac{WK}{N}}/2 + 12e^{-\frac{WK}{2N}}\sqrt{N/2} < N/2e^{-0.8\frac{WK}{N}}$$

. The last inequation holds for $\frac{WK}{N} < 5$, which is enough for our purpose. We thus assume that at most 2^{-128} such sets of W trackers miss more than X stirs, and they would be infeasible to find. Thus the total fraction of stirs that can be evaded is $X/(N/2) = e^{-0.8\frac{WK}{N}}$, and so is the maximum fraction of honest proposers that miss W trackers, which is upper bounded by α. Solving $\alpha = e^{-0.8\frac{WK}{N}}$ we obtain the proposition statement. □

For $N = K^2 = 2^{14}$ we have $W(\alpha) = -160\ln\alpha$.
Now note the following

- The anonymity set of each tracker increases with each honest stir it undergoes.
- Denote the fraction of 1-touchers after r rounds by $F_1(r)$. Since honest and online proposers are uniformly distributed over rounds thanks to the final filtering, and as the Feistel rule is uniform (see Proposition 2), we have

  $$F_1(r) \approx 1-(1-\alpha)^r.$$

  This approximation is good enough for the anonymity set estimate.
- Thanks to the uniformity of dispersion, we have each stir of round $r+1$ taking the same fraction of 1- and 0-touchers. Therefore out of $(1-\beta)K$ benign trackers we have $F_1(r)(1-\beta)K$ 1-touchers each with anonymity set at least $(1-\beta)K$, and the anonymity set of 1-touchers last touched at round $r+1$ is at least

  $$A_1(r+1) = (1-(1-\alpha)^r)(1-\beta)^2K^2$$
- For 1-toucher to be last touched in round r, it must undergo no honest stirs after that, which happens with probability $(1-\alpha)^{s-r}$. Thus the fraction of trackers last touched in round r is $F_2(r) = \alpha(1-\alpha)^{s-r}$.

Proposition 4. *Suppose that the attacker shuts in day 2 down all nodes that were last touched in round r or earlier of day 1. Then the cost is*

$$C(r) \geq \sum_{k=1}^{r} A_1(k)F_2(k)N = \sum_{k=1}^{r}(1-(1-\alpha)^{k-1})\alpha(1-\alpha)^{s-k}(1-\beta)^2K^2N. \tag{1}$$

Theorem 1. *Let the adversary*

- *control βN proposers in period i (i.e. she knows the shuffles of those).*
- *be able to shut down arbitrary δN proposers in period i.*

Let the fraction γ of honest proposers of each day go offline. Then the fraction of honest proposers of each day is $\alpha = 1-\beta-\gamma-\delta$ and the cost of the attack is $C(r_0)$ where

$$r_0 = \log_{1-\alpha}(1-\delta+\frac{W(\alpha)}{2N})$$

Proof. In day 1 the fraction of honest and alive proposers who stir is $\alpha = 1-\beta-\gamma-\delta$. By Lemma the maximum number of trackers that become 0-touchers is $W(\alpha)$, of which 1/2 goes to Day 2. Therefore, out of δN attacked trackers in Day 2, at least $\delta N - W(\alpha)/2$ are 1-touchers. The attacker then shuts down the 1-touchers that were touched at round r_0 at latest such that

$$\sum_{k\leq r_0} F_2(k) \geq \delta - \frac{W(\alpha)}{2N}$$

which is equivalent to

$$\sum_{k\leq r_0} F_2(k) \geq \delta - \frac{W(\alpha)}{2N} \Leftrightarrow \tag{2}$$

$$\sum_{k\leq r_0} \alpha(1-\alpha)^{s-k} \geq \delta - \frac{W(\alpha)}{2N} \Leftrightarrow \tag{3}$$

$$\alpha(1-\alpha)^{s-r_0}\frac{(1-\alpha)^{r_0}-1}{-\alpha} \geq \delta - \frac{W(\alpha)}{2N} \Leftrightarrow \tag{4}$$

$$(1-\alpha)^{s-r_0} - (1-\alpha)^s \geq \delta - \frac{W(\alpha)}{2N} \Leftrightarrow \tag{5}$$

$$r_0 = s - \log_{1-\alpha}\left(\delta - \frac{W(\alpha)}{2N} + (1-\alpha)^s\right) \tag{6}$$

The cost is then $C(r_0)$. □