Privacy of Genomic Data Sharing Beacons: Attack and Protection

Peifeng Hu
EECS Department
Case Western Reserve University
Cleveland Ohio USA
pxh257@case.edu

Qiwen Luo
EECS Department
Case Western Reserve University
Cleveland Ohio USA
qxl216@case.edu

ABSTRACT

The rapid progress of the analysis of human genomic sequences boosts biomedical research that involves large amounts of data. However, with the continuous increase of convenience and decrease of expense to access human genomic sequences, the databases that contain these genomic data are suffering from more attacks. The purpose of this research is to introduce the main attack, Optimal Attack, to the genomic data sharing Beacon system and compare the power of the attack under non-flipping method and Real Time Flipping (RTF) method. This report will also explain how RTF is implemented in the Beacon system under the Optimal Attack and discuss the significance of RTF.

KEYWORDS

Beacon, Real-Time Flipping Protection, Optimal Attack, Data Privacy

1 Introduction

Nowadays, many people have been benefited by privacy-enhancing techniques (PETs) in such an information-explosive era with countless attacks. Real-time Flipping (RTF) method, as one of these PETs, does make a great contribution to limit the amount of leaked information and guarantee the utility of applications. In this report, RTF will be implemented in the scenario with the Optimal Attack, which is a common attack existing in the Beacon system. This report first gives readers a general picture of the mechanisms of the Optimal Attack and RTF. Then the report explains how RTF defends against the attack. Finally, the significance of the RTF in the Beacon system is discussed.

2 Literature Review

In this section, we do a literature review on papers about the Beacon system, the Optimal Attack and Real-time Flipping (RTF) method. We introduce the Beacon system, describe the mechanism of the Optimal Attack and explain how the RTF method is implemented in the Beacon system.

2.1 Beacon system

With the development of techniques to analyze genomic data, DNA sequences can be further illustrated with low cost. These advanced techniques allow more researchers to do research based on genetic data. To enhance data sharing in the biomedical field, the GA4GH established the Beacon system in 2014, which is a search engine designed to assist researchers in locating relevant datasets. This new system greatly facilitates research with regard to human genomic sequences.

Before the development of the Beacon system, as shown in *Figure 1,* researchers who wanted to retrieve useful genomic information had to go through time-consuming processes, involving different middlemen. As for those middlemen, they may not employ professionals to guarantee the privacy of the data, thus, making that data vulnerable. Therefore, the existence of the Beacon system greatly helps secure genomic information. By using the Beacon system, users can get most of the data that they want. As shown in *Figure 2,*

the Beacon system works by accepting yes-or-no queries from users, such as "Whether or not you have the genome with X" where X is a specific feature. And the users will receive "yes" with a link to these data or "no" [1].

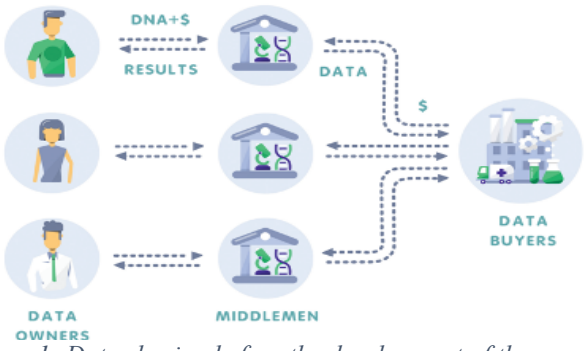

Figure 1: Data sharing before the development of the Beacon system

Figure 2: Data sharing after the development of the Beacon system

2.2 Optimal Attack

Because of the importance of the genomic data, some attacks, such as inference attacks, occur. Some malicious users successfully infer some sensitive information with the help of inference statistic tools, like the log-likelihood ratio test. The goal of the attackers is to link anonymous records to the identity of the individual and to infer whether or not an individual is in the dataset [2] ,[3] .

The Optimal Attack is one of the inference attacks and has already existed for decades. Although there are lots of advanced versions of inference attacks, the Optimal Attack is still an important basis for them. Therefore, the mechanism of the Optimal Attack should be discussed in order to have a general idea of how the Beacon system is attacked. The following three steps talks about how the attack works from the Beacon system's view in detail.

Step 1: Assume that there are 100 people in the database. And the Beacon system consists of 65 randomly chosen people from the database. Then we again randomly choose 20 people from the Beacon system to be the control group. Finally, we randomly pick up 20 people from the database to be the case group. These 20 people in the case group are not in our Beacon.

Step 2: Assume that there is a query q sent by a user. For each person in the case group, the attackers calculate the lambda (Equation 4[1]) which is measured by log-likelihood ratio test (LRT) statistics (Equation 1[1]). The null hypothesis (H0) indicates the possibility that the individual is not in the Beacon. The alternative hypothesis (H1) indicates the possibility that the individual is in the Beacon. The log-likelihood under the null and alternative hypothesis has been defined as Equation 2[1] and Equation 3[1] Since we assume that the attackers are 95% confident that they are correct, we find t_α such that only 5% people whose LRT statics are below that value. That is to say, for these 5% people, the attackers believe that they are in the Beacon.

$$L(R) = \sum_{i=1}^{n} x_i \log(\Pr(x_i = 1)) + (1 - x_i) \log(Pr(x_i = 0)) \quad (1)$$

$$L_{H_0}(R) = \sum_{i=0}^{n} x_i \log\left(1 - D_N^i\right) + (1 - x_i) \log\left(D_N^i\right) \quad (2)$$

$$L_{H_1}(R) = \sum_{i=0}^{n} x_i \log\left(1 - \delta D_N^i\right) + (1 - x_i) \log\left(\delta D_N^i\right) \quad (3)$$

$$\Lambda = L_{H_0}(R) - L_{H_1}(R) \quad (4)$$

Step 3: Because we do not know who is the victim, we assume that everyone in the control group is vulnerable. Thus, for each person in the control group, we calculate the lambda with Equation 4[1]. For those individuals whose lambda is smaller than $t\alpha$, the attackers will reject the null hypothesis. Since the attackers believe that these people are in the Beacon,

the attackers make right prediction on these people. That is to say, these people are attacked.

2.3 Real-time Flipping (RTF)

RTF method is a PET developed in 2018 from a previous flipping method. It attempts to hide some rare variants in the database: when a user asks about the variant, the answer will be no, not yes [4] . The difference between RTF and other flipping methods is that it can guarantee the same level of privacy by flipping fewer responses. It achieves this goal by using p-value in the log-likelihood ratio test to trace the real-time vulnerability of the individual in the Beacon system. Although RTF performs better than other flipping methods, it still permanently hides some rare data, which are important to biomedical research. The workflow (*Figure 3a* and *Figure 3b*) for the PETs is followed with a brief explanation.

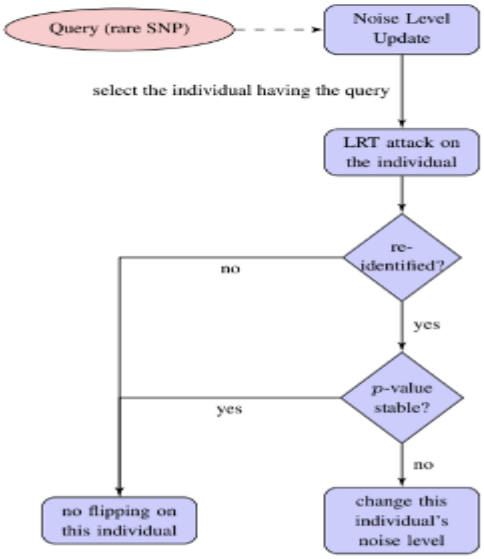

Figure 3b The Workflow for RTF

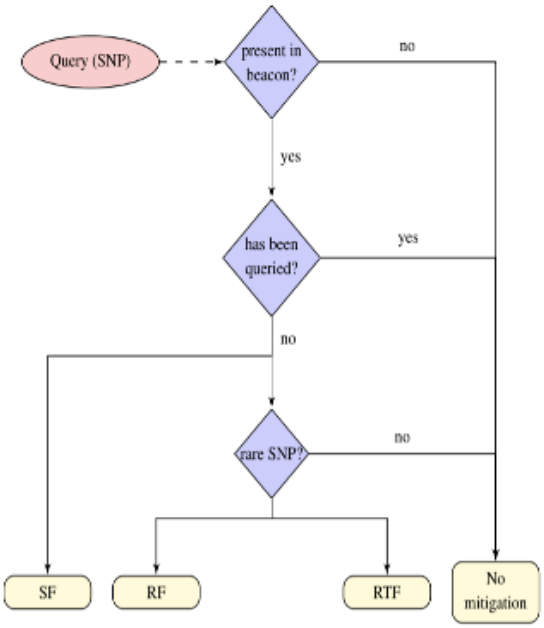

Figure 3a The Workflow for the PETs

Clarification: The control group in RTF contains people who are not in the Beacon.

Step 1: Assume that a user input a query q. If the query has been asked, the Beacon will return the same answer as before. If the response is "no", the Beacon will return "no". Else, RTF will compute the power of the attack, just the same as the mechanism of attacks mentioned above, for each person in the control group based on the current and previous queries.

Step 2: RTF will compute the power of the attack for people in the Beacon. The p-value for each person is the percentage of people in the control group whose power is smaller than him/her. If the p-value is any of person in the Beacon is smaller than 5%, RTF will flip the response. That is to say, the response will be "no" instead of "yes". By flipping the response, the Beacon will hide these particular data from the attackers forever.

3 Experiments and Results

In this section, we describe the experimental setting and the comparison results from two evaluation criteria: re-identification risk and the data utility.

3.1 Experiments

For this research, we conduct two trials, the Optimal Attack under non-flipping method and under RTF method.

3.1.1 Optimal Attack under Non-flipping Method

In order to testify the efficiency of the Real-time flipping method, we first conduct an experiment on the Optimal Attack under the non-flipping method. This trial can be divided into three parts. First of all, we evenly split the database into two groups and one of the groups is considered as the Beacon system. Then we randomly choose 40 individuals from the Beacon system to consist of the control group. Next, we randomly pick up 40 individuals from another group to build the case group. Limited by the performance of our computers, we randomly choose the same 2,000,000 SNPs out of 4,000,000 SNPs for each group.

In this experiment, we send the 1,033 queries to the Beacon system and get the corresponding responses. The responses indicate whether or not there exist some individuals who have a mutation on the given SNP. Then, we calculate lambda for the 40 individuals in the case group with the log-likelihood ratio test. The higher the lambda is, the more probable that the individual is not in the beacon. Ideally, any individual with lambda smaller than the smallest lambda in the case group should be considered in the beacon. However, the attacker in the Optimal Attack is only 95% confident about his LRT statics. Therefore, we set a $t\alpha$ and there are just 5% individuals in the case group whose lambda is below that value. For these individuals, we reject the null hypothesis and believe that they are in the beacon. Namely, they are attacked. After each query, we will calculate the power which indicates the portion of individuals who are attacked.

3.1.2 Optimal Attack under Real-time Flipping Method

The basic idea of RTF is to protect the victim from the re-identification attack by flipping some responses from 1 to 0 since the release of these responses will largely increase the vulnerability of the victim. In order to make RTF effective and get the response in a short time, the vulnerability check only works on the first-time query rare SNPs. If the query has been queried before or it is not a rare SNPs, the Beacon system does not activate RTF, and it simply returns the historical record or the correct answer as a response. In the RTF process, whether the query response needs to be flipped is determined by the p-value. P-value is the percentage of LRT scores in the control group equal to or smaller than that of the target individual. Since the Beacon system does not who is the victim, we assume everyone in the beacon is a target individual, and the one with the lowest LRT value is the most dangerous one. If the p-value is less than 0.05, which means the individual vulnerability is high, then the response is flipped.

3.2 Evaluations

After having conducted the two experiments, the results of them are compared and discussed.

3.2.1 Evaluations on Optimal Attack under Non-flipping Method

Reidentification Risk

According to *Figure 4*, the power curve of the Optimal Attack under RTF method maintains around 0.3 and it is far lower than the power of the attack under non-flipping method. Within the current 1,033 total query question, the RTF method has already decreased the attack power by more than 60 percent. Therefore, we predict that, the attack power with the restrain from RTF method will grow much lower than power of the attack without any PET if we continue asking more queries. Although the power of the attack under RTF method will finally reach 1, but it will need much more queries. Since the attackers generally have limited information that is needed to construct queries, chances are good that they can only attack some of the individuals in the Beacon system before they finish sending all queries. So, based on this diagram, we make the conclusion that with the RTF, the target individual's information in the Beacon system can be protected from the most Optimal Attacks.

Besides the main trends of these two power curves, there exist some fluctuations. The frequent fluctuations are attributed to the special condition that if for the current query question, the LRT scores of most of individuals are very close or even the same, then the confidence range might not be 95%. In this case, t_α might not be exact 95%. We predict those fluctuations

will disappear if we enlarge the query size to be 10 times more than the current query size.

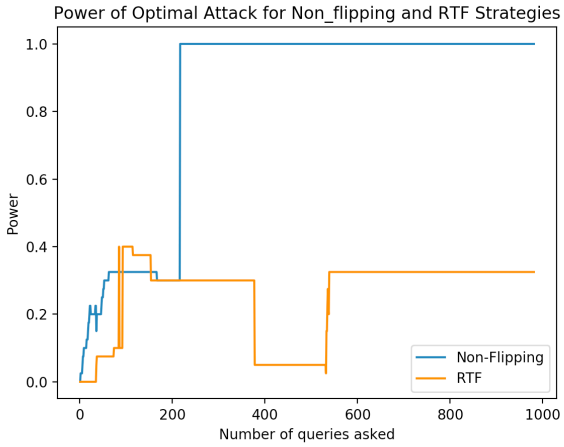

Figure 4 Power of Optimal Attack for Non-flipping and RTF Strategies

The Number of Flipped Queries

According to *Figure 5a* and *Figure 5b*, it is clear to see that the number of flipped response under RTF method is relatively smaller than those under Random Flipping (RF) method and Strategic Flipping (SF) method. The decreasing number of flipped queries should be contributed to the better criteria of which queries should be flipped. As for RF method, it simply flips a random portion of responses and some responses just contain little sensitive information. What's worse, it may not flip some responses which enable attackers immediately make right prediction on the existence of victims. With regard to SF method, although it realizes the importance of differential discriminative power based on the background knowledge of attackers, it ignores how the responses of previous queries affect the attackers' prediction. Therefore, the SF method still flips more responses than necessary. However, RTF method combines the background knowledge with the responses of previous queries. Thus, the number of flipped responses under RTF is far less than those under RF method and SF method as more queries are asked. Because of the time issue, in our research, we didn't query the same number as in the original research paper. But we can still see the tendency that the flipped responses will be fewer even after sufficiently large size of queries.

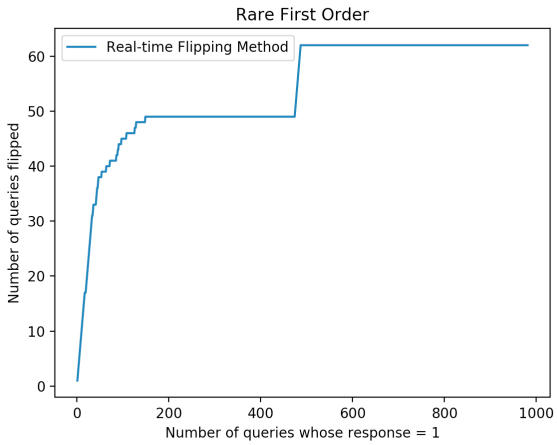

Figure 5a Number of flipped queries under RTF

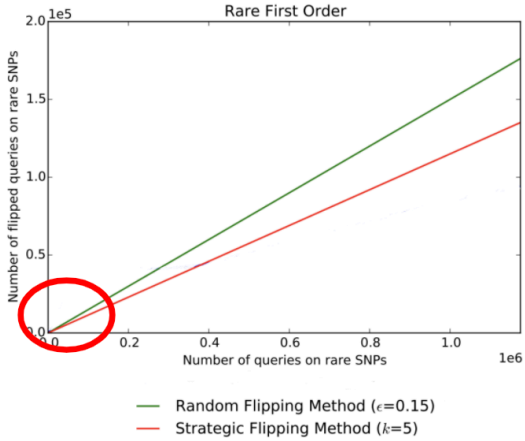

Figure 5b Number of flipped queries under RF and SF

Utility

The utility is determined by the percentage of the flipped answer. Namely, if fewer answers are flipped, the Beacon system has higher utility. The flipped answer will decrease the individual's vulnerability. After the vulnerability is low enough to protect the most individuals in the Beacon system, it is no longer needs to flip more queries. The flip at that time cannot provide higher privacy but hurt the utility. Therefore, the Beacon system will start to return correct responses. According to *Figure 6,* the utility starts from zero and keeps going up to 90% after asking 200 queries. The low utility at the initial stage is because we query rarer SNPs first and they contain too much sensitive information. If we release the information, the individuals in the Beacon system will be attacked with fewer queries asked. By concealing the information, the privacy of some individuals is boosted. With more

questions are queried, the utility finally increases to over 90%, which is a pretty good utility level for the Beacon system. Since for the individuals in the Beacon systems, flipping a few responses is enough to protect their privacy, there is no need to flip all queries whose responses are yes. That is why, the utility will continue going up and approach 100%. Thus we then conclude that RTF method is able to find a balance point between utility and privacy.

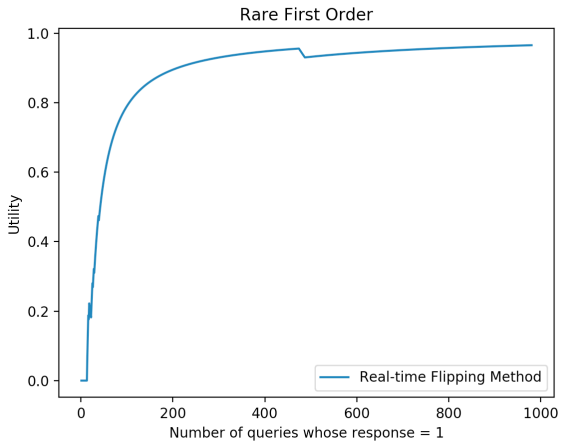

Figure 6 Utility under RTF

4 Significance

In this section, we discuss the significance of the PETS for the Beacon system and the reason why the Real-time Flipping method is more effective than flipping methods.

4.1 The importance of PETs to the Beacon system

With the development of techniques to analyze genomic data, DNA sequences can be further illustrated with low cost. These advanced techniques allow more researchers to do research based on genetic data. To enhance data sharing in the biomedical field, the GA4GH established the Beacon system in 2014, which is a secured information center to store genomic data. The Beacon only allows to answer the queries with regard to the allele-presence information. Therefore, data holders are supposed not to concern data privacy issues [5] .

However, recent studies show that it is probable to decide whether or not the individual is in the Beacon, by querying the Beacon for his/her SNPs for several times [6] . With the re-identification attack, the privacy of the individual in the anonymous-access beacon is susceptible [5] . Some researchers have proven that first-degree relatives and individuals can be identified in the 1000GP. They also demonstrated that they can re-identify a single genome from PGP3 participants by querying the existing beacons 1000 times [5] .

Because of the potential risk to the Beacon system, some PETs have been developed. By sacrificing some utility, these PETs manage to further guarantee the privacy of the Beacon. Among all these PETs, flipping methods are the popular choice. According to the recent research, Random Flipping Method, as a basic version of flipping method, is able to limit the power of the rare-first attack to 0.35 by flipping 15% responses [1].

4.2 Real-Time Flipping Method

Flipping method, one of the popular beacon privacy protection method, has been divided into many different child methods. Among all of the existed flipping methods, the reason why this report introduces RTF is that RTF is a more effective PET compared with other flipping methods for the Beacon.

As for the ability to defend against the re-identification risk, RTF performs better than other flipping methods on randomly ordered rare first ordered, discriminative first ordered and typical user ordered queries [1]. For the Beacon implemented RTF, the risk will be limited to an acceptable level until ~ 120, 000 rare SNPs are queried [1]. However, for the same Beacon implemented Random Flipping (RF) Method and Strategic Flipping (SF) Method, the maximum SNPs queried are around 1,000. As for the utility of the Beacon after utilizing PETs, RTF manages to flip fewer responses than RF and SF under different order of queries [1].

Although RTF performs better than other flipping methods, it still permanently hides some rare data, which are important to biomedical research. This limitation can never be eliminated since the mechanism of flipping methods is to flip some response and, thus, the data related to these responses will be concealed. Because of the constraint in RTF, this research focuses on comparing RTF with developed or new methods.

The comparison can provide some ideas for future development on PETs.

5 Conclusion

In our research, we introduce the Optimal Attack and explain how RTF is implemented in the Beacon system. RTF focuses on enhancing privacy by flipping responses of queries for highly sensitive variants. It performs better than other flipping methods, such as RF and SF, under the Optimal Attack. But the limitation of RTF can never be eliminated since the mechanism of flipping methods is to flip some response and, thus, the data related to these responses will be hided. Under most of circumstances, these data are useful to researchers. Namely, flipping methods always hide some useful information, which may be a loss to researchers.

Given on the fatal flaws of flipping methods, in future research there are some possible technical extension. The researchers can choose to add noise to the Beacon system. Or the researchers can utilize game theory to determine the balance point between high utility and privacy.

REFERENCES

[1] D. Bu, X. Wang, and H. Tang, “Real-time Protection of Genomic Data Sharing in Beacon Services,” AMIA Jt Summits Transl Sci Proc, vol. 2017:45-54, pp. 45–54, May 2018.

[2] E. Ayday and M. Humbert, “Inference Attacks against Kin Genomic Privacy,” IEEE Security & Privacy, vol. 15, no. 5, pp. 29–37, 2017.

[3] J. L. Raisaro, F. Tramèr, Z. Ji, D. Bu, Y. Zhao, K. Carey, D. Lloyd, H. Sofia, D. Baker, P. Flicek, S. Shringarpure, C. Bustamante, S. Wang, X. Jiang, L. Ohno-Machado, H. Tang, X. Wang, and J.-P. Hubaux, “Addressing Beacon re-identification attacks: quantification and mitigation of privacy risks,” Journal of he American Medical Informatics Association, vol. 24, no. 4, pp. 799–805, 2017.

[4] “Global Alliance for Genomics and Health,” Wikipedia, 15-Oct-2019. [Online]. Available: https://en.wikipedia.org/wiki/Global_Alliance_for_Genomics_and_Health. [Accessed: 06-Mar-2020].

[5] X. Shi and X. Wu, “An overview of human genetic privacy,” Annals of the New York Academy of Sciences, vol. 1387, no. 1, pp. 61–72, 2016.

[6] N. V. Thenen, E. Ayday, and A. E. Cicek, “Re-identification of individuals in genomic data-sharing beacons via allele inference,” Bioinformatics, vol. 35, no. 3, pp. 365–371, 2018.