The Power of Refresh: a Novel Mechanism for Securing Low Entropy PII

Yuqian Li, Yang Liu, Zhifang Liu, Zhen Chen
Department of Computer Science and Technology
Tsinghua University
Beijing 10084, China
{*liyuqian79, lywander, chimneyliu*}*@gmail.com, zhenchen@tsinghua.edu.cn*

***Abstract*—Deterministic encryption for low entropy personally identifiable information (PII) is vulnerable to dictionary attack. It is particularly so because of an expedient method to enumerate possible PII's plain text instead of all possible keys. Deterministic encryption, however, is indispensable in the generation of hash or index of PII.**

This paper briefly presents a novel mechanism to frustrate dictionary attacks by refreshing the encryption in an external blackbox. The major part of this paper is about the analysis of this novel mechanism. The use of conditional entropy in this paper both measures the increased difficulty for attack and proves the value and feasibility of this novel mechanism. A lower bound for conditional entropy against a computationally-unbounded adversary is guaranteed. The essential meaning of the lower bound is also given based on min-entropy.

***Keywords*-personally identifiable information; online social network; conditional entropy; deterministic encryption; security;**

I. Introduction

Personally identifiable information (PII) often has a very low entropy (e.g. cellphone numbers) for human memorization. In online social network (OSN), PII is the information to identify a particular user, such as the usernames like cellphone numbers, email addresses. As OSN become more and more popular, protecting PII leakage from both social network operators (SNO) and other users is more important than ever.

OSN could use deterministic encryption of PII, because it both protects the plain text and provides quick identification and indexing. Although seems to be safe, deterministic encryption is vulnerable to dictionary attacks, especially on a level that is independent on SNO. To put it simple, the online identification system explicitly allows for dictionary attack, because the system can hardly tell the difference between a normal human behaviour and a carefully designed automatic brute force dictionary attack. A dictionary attack that simulates normal human behaviour and enumerates all possible values of PII's plain text is feasible unless the encryption schema changes. But a change of encryption schema is impossible for both cost and user-convenience considerations.

Once the dictionary attack has enumerated all possible values of PII's plain text and established a table which maps all cipher texts to corresponding plain texts, the conditional entropy [1], [2] which measures the uncertainty of the plain text given its corresponding cipher text and that table, is 0. Even for high entropy PII, a computationally-unbounded adversary could establish that table and the conditional entropy drops to 0 again. So conditional entropy given all information achieved by adversary during attacks could be a better measurement of the security.

Therefore, a lower bound for conditional entropy can possibly ensure the security, even for low entropy PII. Based on a defender model, a defender mechanism is designed and implemented in an OSN system which uses cellphone numbers to identify users and establish social networks. The analysis of the mechanism shows that a lower bound of conditional entropy can be guaranteed efficiently: suppose that the original entropy is D, a lower bound of conditional entropy $\Omega(D)$ can be guaranteed by performing one defend operation after $2^{\Omega(D)}$ possible attacks. Experiments confirm that our lower bound is valid. Finally, based on min-entropy, the expected chance to guess the right plain text is only $2^{-\Omega(D)}$ for a computationally-unbounded adversary.

The rest of this paper is organized as follows. Section II provides a brief literature review on privacy problems in OSN and entropic security. Section III introduces the defender model and mechanism. Section IV provides a proof as well as experiments and its essential meaning.

II. Related Work

A. Privacy Problems in Online Social Network

Following related works are focused on two privacy problems which we want to solve in a different way for low entropy PII.

Firstly, security of online PII becomes an important concern [8], [9] because of the growing popularity of OSNs, such as Facebook and the growing tendency for users to share their information on OSNs. Meanwhile, more and more users become aware of that security based on well performed management and shielded servers is not reliable since human mistakes, behavior of operators and server vulnerabilities are unpredictable.

Buchegger et al.[10], [11] proposes the use of distributed social networks to control access and remove security dependence on both the SNO(Social Network Operators) and other users. The same purpose could be achieved by traditional

centralized server/client model to preserve the simplicity and performance, such as [12] proposes. In this paper, a novel mechanism based on centralized server/clients is proposed to make a social network with low entropy PII (e.g. cellphone numbers) secure and trusted independent of both SNO and other users.

Secondly, traditional websites tend to encrypt only password of users in their database, but store plain text of PII. However, as more and more new OSNs emerge every day, PII also worth being encrypted as well as password, otherwise one OSN could be easily threatened by another OSN's PII and password leakage. [13] explains the importance of protecting the confidentiality of PII and impacts of PII leakage in the context of information security. It also includes a list of confidentiality safeguards ranging from operational activities to technical methods. Among these safeguards, some researches focus on how to minimize the use and collection of PII. For example, [14] points out two defects in privacy policies of popular OSNs and provides a method to find the minimum of private information needed for a particular set of interactions. In addition, [15] carries out a detailed analysis on possible ways of PII leakage via OSNs. Our work, which is a different approach, is based mainly on another two of the methods listed in [13], i.e. de-identifying information and anonymizing information. With the combination of these two ways, prevention of leakage is no longer necessary, since neither third-party services nor the first-party (the party that directly serves the user) server is able to retrieve plain or recoverable PII data.

B. Entropy and Entropic Security

Entropy[3] measures the uncertainty of an information. Intuitively, it's easy to understand: the cipher text is regarded as secure if the adversary is uncertain about the plain text.

Entropic security is introduced by Russel and Wang[4] to define whether the cipher text leak any predicate of the plain text. However, it requires messages to have high entropy from the adversary's point of view. Similar entropic condition had been achieved in hash functions by Canetti et al[5], [6]. Hash functions are considered to be equivalent to deterministic encryption discussed in this paper: anyone could get a deterministic cipher text from a given plain text, but it's hard to find the corresponding plain text for a given cipher text. Entropic security has been further studied by [7] and its result applies to both encryption and hash functions.

However, all of their work only apply to high entropy messages. While for low entropy message, one simple contradiction has already been shown: enumerate all possible plain texts and a successful collision will recover the original plain text easily.

The key to this failure is the conditional entropy. Mutual information $I(X,Y)$ is widely used in those previous researches. By definition,

$$I(X,Y) = H(X) - H(X|Y) \tag{1}$$

where $H(X)$ is the entropy of X and $H(X|Y)$ is the conditional entropy of X given Y (See definition 1, 3). In their work, X is the plain text and Y is the cipher text. Whether $I(X,Y)$ is small is key to the security they defined. Note that $I(X,Y)$ is small is equivalent to that $H(X|Y)$ is large so $I(X,Y)$ itself does not have any problem. The problem is what Y is. If Y is only the cipher text, it's not suitable for the case that $H(X)$ is small. In the low entropy cases where the adversary could easily launch dictionary attacks, the information from these attacks is critical to the security. Therefore, Y should contain the information from those attacks for a better security analysis.

In summary, conditional entropy $H(X|Y)$ or equivalent mutual information $I(X,Y)$ has already been utilized in previous work. In their work, Y only contains the information of cipher text, while in this paper, Y is defined to contain the information gained by adversary during the dictionary attacks so a better analysis for low entropy encryption is achieved.

III. Defender Model and Mechanism

A. Defender Model

The defender model is a simple model that is not based on formal information theory. In this model, the adversary is called attacker who can launch attacks. After each attack, some useful information is gained. Once enough information is achieved by attacker, the security is compromised.

Initially, the attacker knows nothing. After each attack, the information gained is described as a function f_A, so define:

$$I_0 = 0 \tag{2}$$

$$I_n = f_A(I_{n-1}) \tag{3}$$

Here $I_i \in [0,1]$ describes the amount of information gained after i attacks: 0 for nothing, 1 for enough information to compromise the security.

For attacker who enumerates all possibilities such as dictionary attacker, the function f_A is quite simple:

$$I_n = f_A(I_{n-1}) = I_{n-1} + c \tag{4}$$

where $c = 1/m$ is a constant depend on m, the number of possibilities to be enumerated. In most situations, m is very large (e.g. greater than 2^{128}) so such an attacker needs too many attacks to compromise the security. Therefore, the system with a large m is secured if the attacker is computationally-bounded.

However, for low entropy PII, m is very small so a defender is introduced against that attacker. The defender's action is also described as a function f_D so the equation(3) becomes:

$$I_n = f_A(f_D(I_{n-1})) \tag{5}$$

which means that defender will reduce the information gained by attacker before a new attack can be made.

For attackers who enumerate all possibilities, a defender who periodically reduces the information gained by attacker in a constant rate will be effective. With that defender, the equation(4) becomes

$$I_n = f_D(I_{n-1}) + c = I_{n-1}/d + c \tag{6}$$

Here $d > 1$ is the rate to reduce the information. It can be easily conducted that:

$$\lim_{n\to\infty} I_n = \lim_{n\to\infty} \sum_{0\le i<n} \frac{c}{d^i} = \frac{d\cdot c}{d-1} \ (d>1)$$

This means that for a small d such as 2, even c is as large as 0.1 and the attacker is computationally-unbounded, security will never be compromised.

B. Defender Mechanism

Inspired by defender model, the defender mechanism is implemented in a specific OSN which generates encrypted indexes from given PII. That PII are cellphone numbers in that specific OSN and the defender mechanism is to prevent attackers from knowing the corresponding cellphone number from its index. The defender mechanism also applies to other PII so cellphone numbers are introduced in this paper only for some concrete analysis and a better understanding.

Define the set of cellphone number as $\mathcal{X} = \{x|x \text{ is a cellphone number}\}$. There's a function $f : \mathcal{X} \to F$ to generate index $h = f(x) \in F$ for a given x. The cellphone number set $\mathcal{X}$ has a very small size about $10^{10} \approx 2^{32}$. For a given index h^*, a simple attacker can enumerate all possible x to see whether $f(x) = h^*$. Therefore, in defender model:

$$f_A(I_{n-1}) = I_{n-1} + c = I_{n-1} + 2^{-32}$$

The defender mechanism is going to fulfil the defender function $f_D(I_{n-1}) = I_{n-1}/2$ by updating indexes. If attacker could track each new index from its old index, there's no loss of information for attacker so it has to make sure that the procedure to update the indexes is untrackable. In the specific OSN, indexes and corresponding encrypted user data entries are stored in server's database. This paper suggests a scenario that attackers(e.g. SNO) already escalated their privilege to root access for both server and database. Therefore, the system has to send indexes and data entries to another secured module and get new indexes and encrypted data entries from that module. The module is implemented in a special hardware (something like TPM, i.e. Thusted Platform Module) that nobody could see what's going on inside the hardware without damaging it in real world. The best strategy is to send all indexes and data entries to that hardware and then retrieve all new indexes and data entries together. By doing that, the attacker loses all information, which means $f_D(I_{n-1}) = 0$. However, the entries in database may be too many for that hardware to store. Therefore, in defender mechanism, two indexes and data entries are sent and retrieved between the database and hardware at a time. After that, the attacker can only guess which new index is from which old index from 2 possibilites. Thus, the equation $f_D(I_{n-1}) = I_{n-1}/2$ is fulfilled.

In short, in defender mechanism, there's a function $g : F \to F$ regenerating new indexes from old indexes. The defender mechanism will randomly choose $h_1, h_2 \in F$ that have not been regenerated yet in each time and generate $h_1', h_2' \in F$ in a way that attacker can't tell whether $h_1' = g(h_1), h_2' = g(h_2)$ or $h_2' = g(h_1), h_1' = g(h_2)$. By doing that, the information like $f(x) = h$ becomes information that there's $1/2$ chance $f'(x) = h_1'$ and $1/2$ chance $f'(x) = h_2'$. Thus $f_D(I_{n-1}) = I_{n-1}/2$ is achieved.

In real system, doing such a defend operation to update whole database after each possible attack costs too much. Therefore, the defend operation is required after m possible attack operations rather than one. Under this new condition, f_D is unchanged, while $f_A(I_{n-1}) = I_{n-1} + c$ becomes $f_A(I_{n-1}) = I_{n-1} + c' = I_{n-1} + m \cdot c$. The m can be tuned in balance of security and the efficiency.

IV. Analysis of Conditional Entropy

This section gives out a proof of the defender mechanism and a demonstration of its security under a computationally-unbounded attacker in information theory.

The first subsection below will demonstrate the definition of entropy and conditional entropy along with some definitions and examples in our context. The second subsection will give a proof to the a lower bound for conditional entropy. In the third subsection, experiments are conducted to evaluate the result. The final subsection will give an essential meaning of our lower bound based on min-entropy.

A. Definition and Examples

In this subsection, a brief definition for entropy and conditional entropy is given along with the formal definition of defender mechanism and its behaviour. Some additional examples are taken to further demonstrate the relation between conditional entropy and the security.

Definition 1 (Entropy): The entropy of a discrete random variable X with possible values $\{x_1, x_2, \ldots, x_n\}$ is

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log p(x_i) \tag{7}$$

where $\log$ refers to $\log_2$ in our context.

Correspondingly, in defender mechanism, define

Definition 2: $\mathcal{X} = \{x_1, x_2, \ldots, x_n\}$ is the set of all possible primary images(i.e. PII, and cellphone numbers in our specific OSN) that index $h_i = f(x_i)$ can be calculated. For convenience, define $n = 2^D$. Suppose h^* is the index that attacker wants to get its primary image $x^* \in \mathcal{X}$ satisfying $f(x^*) = h^*$. The discrete random variable X is the primary image guessed by the attacker against x^*.

In ideal situation, the attacker has no related information, so X should be uniformly distributed:

$$H(X) = -\sum_{i=1}^{2^D} 2^{-D} \log 2^{-D} = D$$

Definition 3 (Conditional Entropy): For a discrete random variable X with possible values set $\mathcal{X}$ and another random variable Y with possible values set $\mathcal{Y}$, the conditional entropy of X given Y is

$$H(X|Y) = \sum_{y\in\mathcal{Y}} p(y)H(X|Y=y) \tag{8}$$

$$= -\sum_{y\in\mathcal{Y}} p(y) \sum_{x\in\mathcal{X}} p(x|y) \log p(x|y) \tag{9}$$

In our context, Y represents the related information achieved by attacker. For example, when attacker has enumerated only one x to get $f(x)$, $Y^{(1)}$ can be defined as:

$$\mathcal{Y}^{(1)} = \{y \mid \exists x \in \mathcal{X}, f(x) = y\}$$

$$\forall y \in \mathcal{Y}^{(1)},\ p(Y^{(1)} = y) = \frac{1}{n} = \frac{1}{2^D}$$

$$p(x|y) = \begin{cases} \frac{1}{n-1}, & y \neq h^* \\ 0, & y = h^* \text{ and } f(x) \neq y \\ 1, & y = h^* \text{ and } f(x) = y \end{cases}$$

Similarly, when attacker has enumerated m different primary images, $Y^{(m)}$ can be defined as:

$$\mathcal{Y}^{(m)} = \{y = \{y_1, y_2, \ldots, y_m\} \mid \exists x_i \in \mathcal{X}, f(x_i) = y_i\}$$

$$\forall y \in \mathcal{Y}^{(m)},\ p(Y^{(m)} = y) = \frac{1}{\binom{n}{m}}$$

$$p(x|y) = \begin{cases} \frac{1}{n-m}, & h^* \notin y \\ 0, & h^* \in y \text{ and } f(x) \neq h^* \\ 1, & h^* \in y \text{ and } f(x) = h^* \end{cases}$$

Therefore, $H(X|Y^{(m)})$ can be calculated as:

$$\begin{aligned} H(X|Y^{(m)}) &= \sum_{h^*\in y} p(y)H(x|Y^{(m)} = y) + \\ &\quad \sum_{h^*\notin y} p(y)H(x|Y^{(m)} = y) \\ &= 0 + \frac{\binom{n-1}{m}}{\binom{n}{m}} \log(n-m) \\ &= \frac{n-m}{n} \log(n-m) \end{aligned}$$

As m increases, the conditional entropy decreases and drops to 0 when $m = n-1$. Consistent with the intuition, the conditional entropy which notifies the security decreases about linearly when m is small compared with n.

B. Proof of a Lower Bound

The key of conditional entropy $H(X|Y)$ is the definition of the condition Y. To make a simple proof, we can simplify the condition Y and preserve the information it contains at the same time. Before defining Y, a formal definition of how defender mechanism behaviours is given. Clear definition of X can be found in definition 2 in the above.

The defender mechanism will allow attacker to do at most m possible attack operations before one defend operation. More specifically, between two operations of updating the indexes, at most m indexes are calculated from primary images(i.e. cellphone numbers). It's formally defined as:

Definition 4 (Defender Mechanism): There are functions $f_0, f_1, f_2, \ldots$ where f_0 denotes the most recent function $f : \mathcal{X} \to F$ to generate an index $f(x) = h \in F$ from primary image x. Besides, f_1 denotes the last one used before update, f_2 for the last but one and so on. There are also functions $g_0, g_1, g_2, \ldots$ where g_i is an update function $g_i : F \to F$ such that $f_i(x) = g_i(f_{i+1}(x))$. Considering the capability of hardware, g_i is designed in a way that attacker knows:

$$\begin{aligned} \{g_i(f_{i+1}(x_1)), g_i(f_{i+1}(x_2))\} &= \{f_i(x_1), f_i(x_2)\} \\ &= G_i(x_1, x_2) \end{aligned}$$

for $n/2$ sets $G_i(x_1, x_2)$. But attacker don't know whether $g_i(f_{i+1}(x_1)) = f_i(x_1)$ or $g_i(f_{i+1}(x_1)) = f_i(x_2)$. Here, G_i are totally random to the attacker.

To better describe the interaction among attacks and defends, candidate sets and collision sets are defined:

Definition 5 (Candidate and Collision Set): Candidate sets are $C_0, C_1, C_2, \ldots$ recursively defined as

$$\begin{aligned} C_0 &= \{h^*\} \\ C_i &= \{h | \exists G_{i-1}(x_1, x_2), g_{i-1}(h) \in G_{i-1}(x_1, x_2) \text{ and} \\ &\qquad G_{i-1}(x_1, x_2) \cap C_{i-1} \neq \emptyset\} \ \ (i \geq 1) \end{aligned}$$

Here h^* is the index that attacker wants to know its primary image x^* such that $f_0(x^*) = h^*$. And collision sets are $K_0, K_1, K_2, \ldots$ where

$$K_i = \{h | f_i(x) = h \text{ is enumerated by attacker and } h \in C_i\}$$

The candidate set C_i can be described as the set of indexes calculated by f_i that are possible to be updated to h^* through $g_0, g_1, \ldots, g_{i-1}$. The collision set K_i is the subset of C_i that is enumerated by the attacker. Since g_i and f_i is random to attacker and a maximum of m indexes are allowed to be calculated using one f_i, the random distribution of $|K_i|$ is only related to $|C_i|$ and has a maximum of m.

Now condition Y will be simply defined as following:

Definition 6 (Simple Condition Y_d): Y_d is a random variable with values set $\mathcal{Y} = \{\alpha, \beta\}$ where $Y_d = \alpha$ means that $|C_d| = 2^d$ and $|K_i| = 0$ $(0 \leq i < d)$. Otherwise $Y_d = \beta$. Here d is a parameter to denote the number of updates that defender mechanism is lucky.

By the definition of conditional entropy,

$$\begin{aligned} H(X|Y_d) &= p(Y_d=\alpha)H(X|\alpha) + p(Y_d=\beta)H(X|\beta) \\ &\geq p(Y_d=\alpha)H(X|\alpha) + 0 \end{aligned}$$

To prove a simple lower bound, three lemmas are proposed. The first one shows a lower bound of $H(X|Y_d=\alpha)$ and the other two for a lower bound of $p(Y_d=\alpha)$. The lower bound of $H(X|Y_d)$ is achieved by putting them together.

Lemma 1: $H(X|Y_d=\alpha) \geq d\cdot(1-\frac{dm^2}{2^D-m+1})$

Proof: When $Y_d=\alpha$, the attacker is unlucky in last d updates and defender mechanism is lucky to expand C_d quickly. In this case, the best that attacker could still know are all relations like $f_d(x)=h$ for $x\in\mathcal{X}$.

In addition, $H(A)\geq H(A|B)$ for any A, B, which simply means that knowing something more can never be a bad thing. Let $A=(X|Y_d=\alpha)$ and B be whether there is any $x\in C_d$ that has been enumerated using $f_0, f_1, \ldots, f_{d-1}$ by the attacker or not. Then

$$\begin{aligned} H(X|Y_d=\alpha) &\geq H(A|B) \\ &\geq p(B=false)\cdot H(A|B=false) \end{aligned}$$

When $B=false$, each $f_d(x_i)=h_i\in C_d$ has an equal chance of $f_0(x_i)=h^*$. Therefore:

$$H(A|B=false) \geq -\sum_{i=1}^{2^d}\frac{1}{2^d}\log(\frac{1}{2^d}) = d$$

For $p(B=false)$, use simple counting method:

$$\begin{aligned} p(B=false) &= \frac{\binom{n-dm}{m}}{\binom{n}{m}} \\ &= \frac{(n-dm)\ldots(n-dm-m+1)}{n(n-1)\ldots(n-m+1)} \\ &\geq (\frac{n-dm-m+1}{n-m+1})^m \\ &= (1-\frac{dm}{n-m+1})^m \\ &\geq 1-\frac{dm^2}{2^D-m+1} \end{aligned}$$

So finally:

$$\begin{aligned} H(X|Y_d=\alpha) &\geq p(B=false)\cdot H(A|B=false) \\ &= d\cdot(1-\frac{dm^2}{2^D-m+1}) \end{aligned}$$

■

To prove a lower bound of $p(Y=\alpha)$, the following fact is used. $(Y=\alpha)$ is equivalent to $\big(|C_d|=2^d$ and $|K_i|=0\ (0\leq i<d)\big)$. Therefore

$$\begin{aligned} p(Y=\alpha) = p(|C_d|=2^d) \\ \cdot p(|K_i|=0\ (0\leq i<d)\setminus|C_d|=2^d) \end{aligned}$$

The following two lemmas are for $p(|C_d|=2^d)$ and $p(|K_i|=0\ (0\leq i<d)\setminus|C_d|=2^d)$ respectively.

Lemma 2:

$$p(|C_d|=2^d) \geq 1-\frac{d\cdot 2^{2d-2}+d\cdot 2^{d-1}}{2^D-1}$$

Proof: $|C_d|=2^d$ means that $G_i(x_1,x_2)\cap C_i\leq 1$ for all $G_i(x_1,x_2)$ $(i\leq d-1)$. Define

$$p(A_i) = p\left((\forall G_i(x_1,x_2), G_i(x_1,x_2)\cap C_i\leq 1)\setminus|C_i|=2^i\right)$$

So

$$p(|C_d|=2^d) = \prod_{i=0}^{d-1} p(A_i)$$

It's obvious that $\forall i<d, p(A_i)\geq p(A_{d-1})$, therefore

$$p(|C_d|=2^d) \geq p(A_{d-1})^d = P^d$$

P here can be easily estimated by counting method as

$$\begin{aligned} P &= \frac{(n-2^{d-1})\ldots(n-2^d+1)\cdot(n-2^d-1)!!}{(n-1)!!} \\ &= \frac{(n-2^{d-1})(n-2^{d-1}-1)\ldots(n-2^d+1)}{(n-1)(n-3)\ldots(n-2^d+1)} \end{aligned}$$

Since

$$\frac{n-2^{d-1}-i}{n-1-2i} \geq \frac{n-2^{d-1}-j}{n-1-2j} \text{ when } i\geq j$$

It can be conducted that

$$\begin{aligned} P &= \frac{(n-2^{d-1})(n-2^{d-1}-1)\ldots(n-2^d+1)}{(n-1)(n-3)\ldots(n-2^d+1)} \\ &\geq (\frac{n-2^{d-1}}{n-1})^{2^{d-1}} \end{aligned}$$

Thus

$$\begin{aligned} p(|C_d|=2^d) &\geq P^d \\ &\geq (\frac{n-2^{d-1}}{n-1})^{d\cdot 2^{d-1}} \\ &= (1-\frac{2^{d-1}+1}{n-1})^{d\cdot 2^{d-1}} \\ &\geq 1-\frac{d\cdot 2^{2d-2}+d\cdot 2^{d-1}}{2^D-1} \end{aligned}$$

■

Lemma 3:

$$\begin{aligned} &p(|K_i|=0\ (0\leq i<d)\setminus|C_d|=2^d) \\ &\geq 1-\frac{m^2}{2^D-2^{d-1}+1} \end{aligned}$$

Proof:

$$
\begin{aligned}
&p(|K_i| = 0\ (0 \le i < d) \setminus |C_d| = 2^d) \\
&\ge p(|K_{d-1}| = 0 \setminus |C_{d-1}| = 2^{d-1})^d \\
&= \left(\frac{\binom{n-2^{d-1}}{m}}{\binom{n}{m}} \right)^d \\
&\ge \left(1 - \frac{2^{d-1}m}{n-m+1} \right)^d \\
&\qquad \text{(see proof of lemma1 for similar conclusion)} \\
&= 1 - \frac{2^{d-1}md}{n-m+1}
\end{aligned}
$$

■

By putting them together, here comes the lower bound

$$
\begin{aligned}
H(X|Y_d) &\ge p(Y_d = \alpha) \cdot H(X|Y_d = \alpha) \\
&= H(X|Y_d = \alpha) \cdot p(|C_d| = 2^d) \\
&\quad \cdot p(|K_i| = 0\ (0 \le i < d) \setminus |C_d| = 2^d) \\
&\ge (1 - \frac{d \cdot 2^{2d-2} + d \cdot 2^{d-1}}{2^D - 1}) \\
&\quad \cdot (1 - \frac{2^{d-1}md}{2^D - m + 1}) \cdot (1 - \frac{dm^2}{2^D - m + 1}) \cdot d \\
&= B(D, m, d)
\end{aligned}
$$

Note that Y_d here contains all information that a computationally-unbounded attacker can achieve after using the system to enumerate (primary image, index) pairs for an infinite long time. Also note that the formula above satisfies arbitrary number d. Thus, the lower bound of $H(X|Y)$ is the maximum value of that formula over all possible d. As a result, this is our final theorem:

Theorem 1: Under defender mechanism, the primary image's conditional entropy has a lower bound of

$$\max_{0 \le d \le D} \{B(D, m, d)\}$$

given all the information that a computationally-unbounded attacker can have in an infinite long time. Here m is the maximum number of indexes that are allowed to be calculated between defend operations and $D = \log(n)$ denotes the logarithm of the size of primary image set.

The formula above is a little complex. A much easier asymptotic result could be derived from that. Suppose that $d = c_1 D, m = 2^{c_2 D}$ $(c_1, c_2 < 1)$ and D is large enough:

$$
\begin{aligned}
H(X|Y_d) &= B(D, m, d) \\
&= \left(1 - \frac{c_1 \cdot D}{2^{D - 2c_1 D + 2}} + o(1) \right) \\
&\quad \cdot \left(1 - \frac{c_1 D}{2^{D - c_1 D + 1 - c_2 D}} + o(1) \right) \\
&\quad \cdot \left(1 - \frac{c_1 D}{2^{D - 2c_2 D}} + o(1) \right) \cdot c_1 D
\end{aligned}
$$

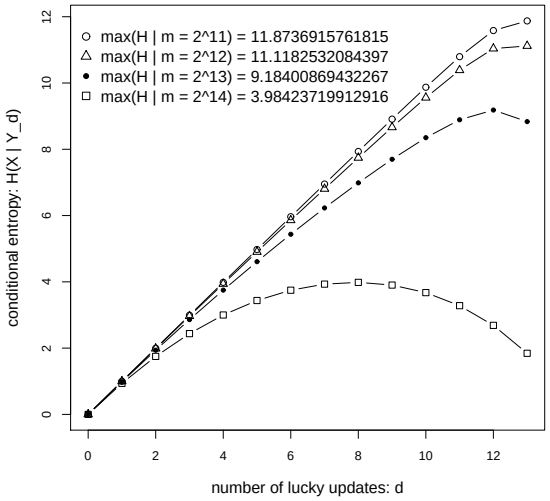

Figure 1. Lower Bound over d

Therefore, when $2c_1, c_1 + c_2, 2c_2 < 1$, for example $c_1 = c_2 = 1/3$, and D is large enough, there exists:

$$
\begin{aligned}
m &= 2^{c_2 D} = 2^{\Omega(D)} \\
H(X|Y_d) &= c_1 D + o(D) = \Omega(D)
\end{aligned}
$$

So the following theorem is derived:

Theorem 2: Under defender mechanism, primary image's conditional entropy has a lower bound of $\Omega(D)$ given all the information that a computationally-unbounded attacker can have in an infinite long time when one defend operation is enforced after $2^{\Omega(D)}$ calculations of indexes. Here $D = \log(n)$ is the logarithm of the size of primary image set.

C. Concrete Lower Bound and Analysis

In our specific OSN dealing with cellphone numbers, $D = 32$. The simple lower bound proved above when $m = 2^{11}, 2^{12}, 2^{13}, 2^{14}$ is given in figure 1.

Since our lower bound in theorem 1 is a maximum value over d, the x-axis is d and the peak of each line is the lower bound for each m. As it shows, when $m = 2^{12} = 4096$, the lower bound is about 11.1. Thus only one update operation after thousands of index calculations is required to guarantee a lower bound higher than 10.

In fact, the proved lower bound in theorem 1 is so simple and the tight lower bound is expected to be much higher for the following reasons. Observing the proof of theorem 1, only the entropy in the situation $Y = \alpha$ is count. However, in many situations that $Y = \beta$, there is still a high entropy. What's more, $B = false$ is also assumed so the attacker is given an extra information about whether all his enumerated x in recent d updates are in candidate set C_d. But in real situation, this is unknown to the attacker.

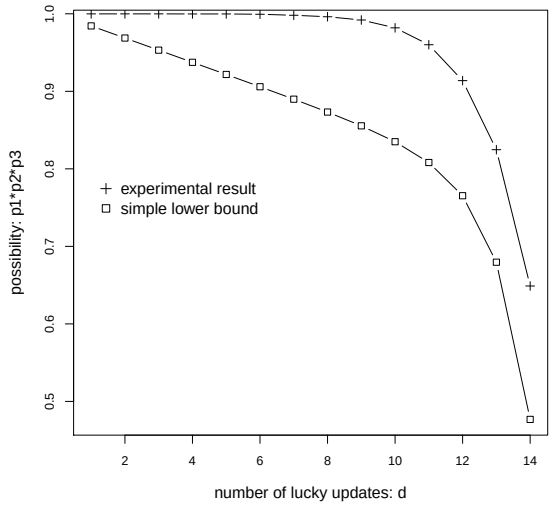

Figure 2. $p_1 \cdot p_2 \cdot p_3$ when $m = 2^{13}$

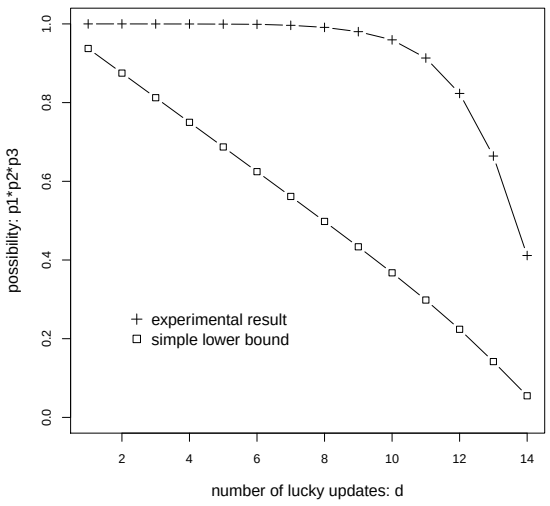

Figure 3. $p_1 \cdot p_2 \cdot p_3$ when $m = 2^{13}$

D. Experimental Evaluation

For convenience, define

$$p_1 = p(B = false)$$
$$p_2 = p(|C_d| = 2^d)$$
$$p_3 = p(|K_i| = 0 \ (i \leq 0 < d) \setminus |C_d| = 2^d)$$

In our proof above, p_1, p_2 and p_3 are three key points to the final result. Lower bound for each of them has been proved and lower bound of $H(X|Y_d)$ is achieved by:

$$H(X|Y_d) \geq p_1 \cdot p_2 \cdot p_3 \cdot d \geq B(D, m, d)$$

In fact, $p_1 \cdot p_2 \cdot p_3$ can be measured in a real program which simulates the same behaviour as defender mechanism. So the proof above can be evaluated by this experiment. Moreover, this experiment will show how tight our lower bound is when $H(X|Y_d = \beta)$ and $H(A|B = true)$ are ignored.

The experiment program simply simulates the whole process of d updates for 10000 times and records the number of successful events to estimate the possibility $p_1 \cdot p_2 \cdot p_3$.

Figure 2, 3 show the result when $m = 2^{13}, 2^{14}$

It can be seen that the simple lower bound is not too far away from the experimental result when $m = 2^{13}$. However when $m = 2^{14}$, the simple lower bound estimated is much smaller than experimental result. Therefore, there is still plenty of room to improve the lower bound to make it tight, even if $H(X|Y_d = \beta)$ and $H(A|B = true)$ are ignored. Meanwhile, the lower bound that can be proved should be higher than we simply get from theorem 1. For example, when $m = 14$, the experimental result of $p_1 \cdot p_2 \cdot p_3$ shows a lower bound of 10 when $d = 11$, while our simple lower bound only shows 4 when $d = 8$.

To check that the simple lower bound is far from the experimental result only for large m, one more experiment is conducted for $m = 2^{11}$ and shown in figure 4 which confirms that our estimation of p_1, p_2, p_3 is correct and accurate for small m.

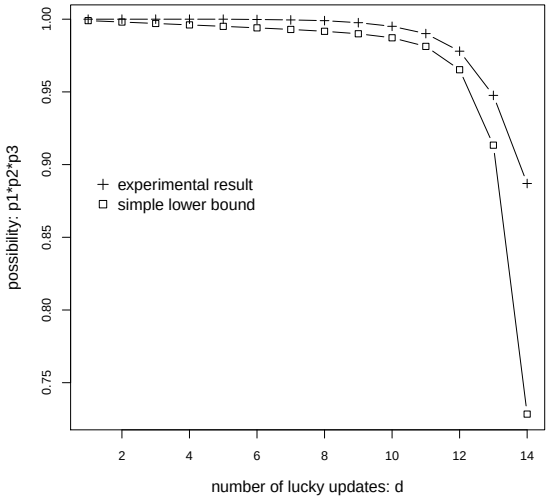

Figure 4. $p_1 \cdot p_2 \cdot p_3$ when $m = 2^{11}$

In sum, it has been evaluated that our simple lower bound is valid while it is not so tight even if we ignore $H(X|Y_d = \beta)$ and $H(A|B = true)$, especially when m is large. In the experiment, it shows that when $D = 32$ and $m = 2^{14} = 16384$, the lower bound is still at least 10.

E. Essential Meaning based on Min-Entropy

All the analysis above is based on Shannon entropy. And min-entropy $H_\infty(X)$ define the entropy in a new way that

$$H_\infty(X) = \min_{x \in \mathcal{X}} (-\log p\,(X = x))$$

Similar conditional min-entropy could also be defined.

The simple proof above also applies to this min-entropy because $p(x|Y=y)$ is either 0 or 2^{-d} which implies:

$$-log(0) = \infty > -log(2^{-d}) = d$$

And the lower bound for Shannon entropy and min-entropy in our proof is the same for the same reason. As it can be seen that min-entropy's definition looks simpler, it's easier to find out the meaning of the lower bound for conditional min-entropy. For min-entropy with a deterministic condition, $H_\infty(X|Y=y) = h$ denotes the highest probability 2^{-h} that adversary can achieve to guess the right answer when $Y = y$ is known. Since $H_\infty(X|Y) = E\left(H_\infty(X|Y=y)\right)$, conditional min-entropy means the expected highest possibility that one adversary can guess the right answer. Therefore, the proof of our lower bound shows that the expected highest possibility that a computationally-unbounded adversary can guess the right plain text is very small: $2^{-\Omega(D)}$. And it's 2^{-10} in the special case for $D = 32$ and $m = 2^{12}$.

Since h is either d or 0 in our proof, $H_\infty(X|Y)$ is

$$\begin{aligned} E\left(H_\infty(X|Y=y)\right) &= p\left(H_\infty(X|Y=y) = d\right) \cdot d \\ &= p_1 \cdot p_2 \cdot p_3 \cdot d \end{aligned}$$

where $p_1 \cdot p_2 \cdot p_3$ is the chance to still confuse the adversary with 2^d equally possible uncertainties.

So as in the graph of $p_1 \cdot p_2 \cdot p_3$ when $m = 2^{11}$ displayed above, both simple lower bound and experimental result show that there is a chance greater than 95% percent that the adversary will be confused with 2^{12} equally possible uncertainties even if he or she is computationally-unbounded and has been attacking for an infinite long time, as long as one defend operation is enforced after 2^{11} index calculations.

V. Conclusion

To ensure the security of deterministic encryption for low entropy PII such as cellphone numbers, this paper briefly presents a novel defender model as well as a defender mechanism implemented for a specific OSN which uses cellphone numbers to generate encrypted indexes. The defender mechanism also applies to PII other than cellphone numbers.

This paper mainly focuses on analysis of this defender mechanism. A lower bound of conditional entropy is calculated to prove the mechanism's security for even computationally-unbounded adversaries. At the same time, the system's efficiency is also kept. Asymptotically, suppose that the original entropy is D, a lower bound for conditional entropy of $\Omega(D)$ can be guaranteed when only one defend operation is required after $2^{\Omega(D)}$ attacks. Based on min-entropy, our proof shows that such an adversary only has an expected chance less than $2^{-\Omega(D)}$ to guess the right plain text. However, the lower bound derived is believed to be not so tight. Conducted experiments confirm that the proved lower bound is valid while the tight lower bound should be much higher even if a lot of things are ignored.

In short, it's theoretically secured and should be more practically secured.

References

[1] G. A. Korn and T. M. Korn, *Mathematical Handbook for Scientists and Engineers: Definitions, Theorems, and Formulas for Reference and Review*. New York: Dover, 2000.

[2] C. Arndt, *Information Measures: Information and its description in Science and Engineering)*. Berlin: Springer, 2001.

[3] C. E. Shannon, "Mathematical handbook for scientists and engineers: Definitions, theorems, and formulas for reference and review," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 5, no. 1, pp. 3–55, 2001.

[4] A. Russel, S. Key, E. Russell, and H. Wang, "How to fool an unbounded adversary with a short key," 2002.

[5] R. Canetti, "Towards realizing random oracles: Hash functions that hide all partial information." Springer-Verlag, 1997, pp. 455–469.

[6] R. Canetti, D. Micciancio, and O. Reingold, "Perfectly one-way probabilistic hash functions."

[7] Y. Dodis, "Entropic security and the encryption of high entropy messages," in *In Theory of Cryptography Conference (TCC) 05*. Springer-Verlag, 2005, pp. 556–577.

[8] A. Rabkin, "Personal knowledge questions for fallback authentication: security questions in the era of facebook," in *SOUPS '08: Proceedings of the 4th symposium on Usable privacy and security*. New York, NY, USA: ACM, 2008, pp. 13–23.

[9] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Commun. ACM*, vol. 50, no. 10, pp. 94–100, 2007.

[10] S. Buchegger and A. Datta, "A case for p2p infrastructure for social networks - opportunities & challenges," in *WONS'09: Proceedings of the Sixth international conference on Wireless On-Demand Network Systems and Services*. Piscataway, NJ, USA: IEEE Press, 2009, pp. 149–156.

[11] S. Buchegger, D. Schiöberg, L.-H. Vu, and A. Datta, "Peerson: P2p social networking: early experiences and insights," in *SNS '09: Proceedings of the Second ACM EuroSys Workshop on Social Network Systems*. New York, NY, USA: ACM, 2009, pp. 46–52.

[12] J. Anderson, C. Diaz, J. Bonneau, and F. Stajano, "Privacy-enabling social networking over untrusted networks," in *WOSN '09: Proceedings of the 2nd ACM workshop on Online social networks*. New York, NY, USA: ACM, 2009, pp. 1–6.

[13] E. McCallister, T. Grance, and K. Scarfone, "Guide to protecting the confidentiality of personally identifiable information (pii)," 2010. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

[14] B. Krishnamurthy and C. E. Wills, "Characterizing privacy in online social networks."

[15] B. Krishnamurthy and C. E. Wills, "On the leakage of personally identifiable information via online social networks."