2A4

秘密の忠告によるオンライン予測

Online Prediction from Private Advice

佐久間 淳[*1*2]
Jun Sakuma

[*1]筑波大学 大学院システム情報工学研究科
[*1]Graduate School of SIE, University of Tsukuba
[*2]科学技術振興機構
[*2]Japan Science and Technology Agency

In this paper, we consider online prediction from expert advice in a situation where each expert observes its own loss at each time while the loss cannot be disclosed to others for reasons of privacy or confidentiality preservation. Our secure exponential weighting scheme enables exploitation of such private loss values by making use of cryptographic tools. We proved that the regret bound of the secure exponential weighting is the same or almost the same with the well-known exponential weighting scheme in the full information model. In addition, we prove theoretically that the secure exponential weighting is privacy-preserving in the sense of secure function evaluation.

1. はじめに

オンライン予測問題とは, 各時刻に複数のエキスパートから与えられる忠告 (予測) に基づいて, 逐次的に生成される次の時刻の事例のラベルを学習者が予測する問題である. 通常オンライン予測では目標とする系列について統計的な仮定を措かない. そのためオンライン予測アルゴリズムの性能は一般の分類問題と異なり regret 関数によって評価される. regret とは, 最もよい予測性能を達成したエキスパートの予測性能と, 学習者の予測性能の差を表す指標である.

学習者が全てのエキスパートが生成する予測とその損失を観測できる場合, これを完全情報モデル (full information model) と呼ぶ. 一方, 学習者が選択した一人のエキスパートからのみ予測と損失を観測できる場合, これを部分情報モデル (partial information model) と呼ぶ. 部分情報モデルは, 学習者-エキスパート間の物理的/通信量的制約のために予測/損失観測が制限される状況を想定している. これに対し本研究では各エキスパートは自身の予測/損失を, 機密性保護のために他のエキスパートや学習者に開示することができないモデルを想定する. 以下に直観的な例を示す.

株価予測問題: ある株式の価格を日に一度予測する N 人の投資家がいる. 各投資家が利用している予測関数の機密性から, 投資家は各々の予測関数や予測価格を外に開示しようとはしない. 一方で, 投資家はほかの投資家の予測を共同して集約し, 予測の精度を向上したいと考えている. 投資家はどのようにすれば予測関数の機密性を侵すことなく, よりよい予測を達成することができるだろうか？

この問題は, 予測/損失情報の観測が制約された中での regret 最小化に帰着される. この例では, 機密性保持のためにエキスパート間で予測/損失情報が共有できないため, 自身が持つ予測関数以上の性能を達成することができない. 一方, もしそのような損失値が持つ情報を, その損失値が他者に公開されたり推定されたりしないような方法でオンライン予測に活用できるならば, このように制約された損失観測下でのオンライン予測であっても, 制約のない損失観測下におけるオンライン予測にせまる性能を達成することができるはずである.

関連研究 N と T をそれぞれエキスパート数と時間ステップ数とすると, 完全情報モデルにおける exponential weighting 法 (後述) の regret は高々$O(\sqrt{T \ln N})$ である [3]. 部分情報モデルにおいては, regret の上界が高々$O(\sqrt{NT \ln N})$ であるような expoenntial weighting 戦略 Exp3 が提案されている [1](表 1).

部分情報モデルにはいくつかのバリエーションが知られ [2], これらの手法は制約された観測下での regret 最小化を目的として設計されているものの, プライバシ保護の理論的な保証を目指しているわけではない. そのため, プライバシ保護の観点からは秘密情報の部分的開示や統計的推測のリスクがある.

本研究では, オンライン予測におけるプライバシを, プライベート情報モデル (private information model) と呼ばれる情報モデルにより定式化する. 直感的には, このモデルでは, 学習者はエキスパートらの, エキスパートは学習者や他のエキスパートらの, 秘密の損失/予測を観測することが許されない.

本稿の構成 2 章ではオンライン予測を導入する. 3 章ではプライベート情報モデルを定義し, このモデルにおけるオンライン予測が, "ルーレット盤面を見ずにルーレットをプレイ"する紛失ルーレットと等価であることを示す. 4 章ではビルディングブロックとして準同形性公開鍵暗号を導入し, 5 章ではこれを用いた紛失ルーレットプロトコルを提案する. また理論解析として, (1) 提案法と完全情報モデルにおける exponential weighting 法の上界の差は $O(1)$ であること, (2) 提案法はプライベート情報モデルの定義において seucre であること, を示す (表 1). 6 章では提案法の計算効率性を確認する実験を行う. 本稿では指数の都合による全ての Lamma と Theorem の証明は省略されている. これらについては [5] を参照されたい.

2. 準備

学習者と複数の**エキスパート** $\mathcal{E} = \{1, ..., N\}$ を考える. オンライン予測の目標は, **環境**から任意に与えられる系列 $y_1, y_2, ...(y_t \in \mathcal{Y})$ の予測である. 本稿では出力空間 $\mathcal{Y}$ は離散であると仮定し, 出力空間を一般性を失うことなく整数の集合 $\mathcal{Y} = \{1, 2, ...Y\}$ として扱う. **完全情報モデル**においては, 学習者は各時刻 t においてエキスパートの**忠告** $\boldsymbol{y}_t = (y_{1,t}, y_{2,t}, ..., y_{N,t})$ を観測可能である. 予測の損失は,

連絡先: 佐久間 淳, 筑波大学大学院システム情報工学研究科, 〒 305-8571 茨城県つくば市天王台 1-1-1, jun@cs.tsukuba.ac.jp

表 1: Regret bound and the information model

online procedure	info. model	regret bound	comp. time	privacy loss
Exponential Weighting (Vovk90)	full	$R_{\mathsf{EW},T} \leq \sqrt{2T \ln N}$	small	not cared
Exp3 (Auer03)	partial	$R_{\mathsf{Exp3},T} \leq 2\sqrt{e-1}\sqrt{NT \ln N}$	small	partly disclosed
SEW with crypto (proposal)	private	$R_{\mathsf{SEW/OR},T} \leq \sqrt{2T \ln N} + c$, $c = O(1)$	medium	none

損失関数 $\ell : \mathcal{Y} \times \mathcal{Y} \mapsto [0,1]$ によって評価される.

エキスパートの予測の**戦略**は確率ベクトル $\boldsymbol{p}_t = (p_{1,t}, ..., p_{N,t})$ で表現される. 学習者は時刻 t において i 番目のエキスパートを確率 $p_{i,t}$ で選択し, i 番目のエキスパートが選んだ予測を自身の予測とする. 学習者は観測した損失に基づいて次の予測のために戦略 $\boldsymbol{p}_t$ を更新する. 以下は完全情報モデルにおけるオンライン予測のプロシージャである.

完全情報モデルにおけるオンライン予測

1. 環境が次の出力 y_t を任意に決定する
2. 各エキスパートは予測 $(y_{1,t}, ..., y_{N,t})$ を学習者に公開する
3. 学習者は観測したエキスパートの予測に基づき予測 $\hat{y}_t = y_{j,t}$ を決定する. ただし $j \sim M(i; \boldsymbol{p}_t)$.
4. 環境は y_t を公開
5. 学習者は損失を評価し, 戦略 $\boldsymbol{p}_t$ を更新し, $t = t+1$ とし step 1 へ

ここで, $j \sim M(i; \boldsymbol{p}_t)$ は, $p_{i,t}$ に比例する確率でランダムに $\{1, ..., N\}$ をサンプルする操作を表す.

H を学習者が戦略の更新に利用するオンラインアルゴリズムとする. i 番目のエキスパートおよびアルゴリズム H の期間 T の損失和をそれぞれ $L_{i,T} = \sum_{t=1}^{T} \ell_{i,t}$, $L_{\mathsf{H},T} = \sum_{t=1}^{T} \ell_{\mathsf{H},t}$ とする. このとき, オンラインアルゴリズム H の**後悔** (regret) は下式で定義される.

$$R_{\mathsf{H},\mathsf{T}} = L_{\mathsf{H},T} - \min_i L_{i,T} \tag{1}$$

学習者の目的は, 所与の期間 T における regret が最小になるように $\boldsymbol{p}_t$ を更新することである. exponential weighting 法 (EW) は以下のように戦略を更新する. $t \geq 2$ について,

$$w_{i,t} = \exp\Big(-\eta \sum_{s=1}^{t-1} \ell(y_{i,s}, y_s)\Big) \tag{2}$$

$$W_t = \sum_{i=1}^{N} w_{i,t}, \quad p_{i,t} = \frac{w_{i,t}}{W_t} \tag{3}$$

ここで $\eta > 0$ はユーザパラメータである. このとき exponential weighting における regret の上界は

$$L_{\mathsf{EW},T} - \min_i L_{i,T} \leq \sqrt{2T \ln N}.$$

で抑えられることが知られている [3].

3. オンライン予測におけるプライバシ

3.1 プライベート情報モデル

はじめにプライベート情報モデルを定義を与える.

Definition 1. *(プライベート情報モデル)* 学習者と N 人のエキスパートにおいて, 全てののパーティー間で予測/損失系列が共有されないとき, これをプライベート情報モデルとよぶ.

続いて, プライベート情報モデルにおけるオンライン予測問題を定義する.

Statement 1. *(プライベート情報モデルにおけるオンライン予測)* H をオンライン予測アルゴリズムとする. 学習者と N 人のエキスパートは時刻 $t-1$ においてプライベート情報モデルを満足している. 時刻 t における H の実行後, 学習者は H から予測を得るが, そのほかには何も得ない. また全てのパーティーは時刻 t においてプライベート情報モデルを満足する.

3.2 接近法

プライベート情報モデルでは, 全てのパーティー間で情報共有が許されない. ただし $w_{i,t}$ は i 番目のエキスパートの損失の系列のみから計算可能なため, i 番目のエキスパートは情報共有なしに独立に式 2 を更新可能である. 一方, $p_{i,t}$ の更新時にはすべての i について $w_{i,t}$ を必要とするため, どのエキスパートも式 3 を更新できない. 従ってプライベート情報モデルにおいてオンライン予測を実現するためには, 学習者は $j \sim M(i; \boldsymbol{p}_t)$ なる $\hat{y} = y_j$ を $\hat{y}_t$ 以外の知識を何も得ずに得るプロトコルを必要とする.

この問題は**紛失ルーレット**と呼ばれる, N 人のディーラーによって分散管理されたルーレット盤を用いた仮想的なルーレットゲームの問題と等価であり, 直感的には以下の性質をもつ.

[紛失ルーレット]

- ルーレット盤は N 個のパーツに分解されている
- ディーラーは一人一つのパーツを管理し, 各パーツにラベルと重みを設定できる
- プレイヤーは, 各パーツの重みに比例する確率でパーツを一つ選び, そのラベルを読むことができる. ただし得たラベルがどのディーラーに書き込まれたかを知ることはできない
- プレイヤーは, その他のパーツについて何の情報も知ることができない
- ディーラーも, プレイヤーがどのパーツを選択したか, どのラベルを読み込んだかを知ることができない

以下に紛失ルーレットゲームの定義を与える.

Statement 2. *(紛失ルーレット)* N 人のディーラーと *1* 人のプレイヤーがいる. i 番目のディーラーは入力 $m_i \in [0,1]$ とラベル $y_i \in Y$ をもつ. 確率ベクトル $\boldsymbol{p} = (p_1, ..., p_N)$ を $p_i = \frac{m_i}{\sum_{i=1}^{N} m_i}$ とする. このとき, 紛失ルーレットの実行後, プレイヤーは $j \sim M(i; \boldsymbol{p})$ なる $\hat{y} = y_j$ を得るが, それ以外は何も得ない. ディーラーもまた何も得ない.

次章に紛失ルーレットを解くための暗号理論的ツールを導入し, 紛失ルーレットを実行するためのプロトコルを導入する.

4. 準同形性公開鍵暗号

準同形性公開鍵暗号 (homomorphic public-key cryptosystem) とは, 暗号値に準同形な演算を許す公開鍵暗号系である. $(\mathsf{sk}, \mathsf{pk})$ を秘密鍵-公開鍵ペア, m をメッセージとする. $c = \mathrm{Enc}_{\mathsf{pk}}(m; \ell)$ は m の (ランダム化された) 暗号化を, $m = \mathrm{Dec}_{\mathsf{sk}}(c)$ は複号化を表す. ここで ℓ が $\mathbb{Z}_Q$ から一様ランダムに選択されたとき, 暗号値 c は $\mathbb{Z}_Q (= \{0, ..., Q-1\})$ 上に一様ランダムに分布するものとする. **加法的準同形性公開鍵暗号**で

Distributed roulette

- The i-th dealer's input: $m_i \in [0,1]$ and $y_i \in \mathcal{Y}$
- The player's output $\hat{y}$

1. Round $k = 1$.
2. For $i = 1, ..., N$, the i-th dealer independently chooses:

$$a_{i,k} \leftarrow \begin{cases} y_i, & \text{with prob. } m_i, \\ Y+1, & \text{otherwise.} \end{cases}$$

   and sends $a_{i,k}$ to the player.
3. The player chooses $j \in_r \{1, ..., N\}$.
   (a) If $a_{j,k} \in \mathcal{Y}$, the player outputs $a_{j,k}$ as $\hat{y}$.
   (b) Else $k \leftarrow k+1$ and go to Step 2.

図 1: Distributed roulette

は, 任意の平文 m_1, m_2 の暗号値について, 秘密鍵の知識なしに暗号値同士の加算および暗号値と整数の乗算が演算 $\cdot$ に基づいて可能である.

$$\begin{aligned} \mathrm{Enc}_{\mathsf{pk}}(m_1 + m_2 \mod N; \ell) &= \mathrm{Enc}_{\mathsf{pk}}(m_1; \ell_1) \cdot \mathrm{Enc}_{\mathsf{pk}}(m_2; \ell_2) \\ \mathrm{Enc}_{\mathsf{pk}}(km \mod N; k\ell) &= \mathrm{Enc}_{\mathsf{pk}}(m; \ell)^k. \end{aligned}$$

以降に示す提案法では, 標準的な暗号理論上の仮定の下で, Paillier 暗号 [4] などの, 強秘匿な加法的準同形性暗号を利用する.

5. プライベート情報モデルのオンライン予測

すでに議論したように, プライベート情報モデルにおけるオンライン予測は紛失ルーレットゲームと等価である. はじめに図 1 に示す分散ルーレット (distributed roulette) ゲームを考える. $a \in_r A$ は, 要素 $a \in A$ の集合 A からの一様ランダムな選択を行う演算を表す. このとき分散ルーレットプロトコルの出力は Lemma 1 に従う.

Lemma 1. *$\hat{y}$ を分散ルーレットの出力とする. このとき, $j \sim M(i; \boldsymbol{p})$ なる j について $\hat{y} = y_j$ (証明略).*

ここでは, 各ディーラが独立に確率 m_i で選択したラベル y_i をプレイヤーが独立に一つ選択することによって, $M(i; \boldsymbol{p})$ からのサンプリングを実現している. このように分散ルーレットはプレイヤーおよびディーラー間で重み m_i を共有しないルーレットゲームを実現するが, プレイヤーは m_i を $a_{j,k}$ の系列から推測可能であり, またプレイヤーは j どのディーラーから $\hat{y}$ が与えられたかを知ることができ, Statement 2 の意味では安全ではない.

5.1 暗号を用いた紛失ルーレット

上記の問題点を考慮し, 準同形性公開鍵暗号を利用した紛失ルーレットプロトコルを提案する (図 2). まず, 紛失ルーレットが分散ルーレットの挙動に近似することを示す.

Lemma 2. *$\hat{y}$ を紛失ルーレットプロトコルの出力とする. また*

$$M'(i; \boldsymbol{p}, N, Q) = (1-\gamma) M(i; \boldsymbol{p}) + \gamma U(i; N). \tag{4}$$

と定義する. ただし $\mu = \frac{\sum_{i=1}^N m_i}{N}$, $U(i; N)$ は $\{1, ..., N\}$ 上の一様分布, Q は暗号系のセキュリティパラメータ, $\gamma = \frac{(1-\mu)\frac{N}{Q}}{1-(1-\mu)(1-\frac{N}{Q})}$ である. このとき $j \sim M'(i; \boldsymbol{p}, N, Q)$ なる j について $\hat{y} = y_j$ である. (証明略)

Oblivious Roulette

- Public input: number of dealers N, security parameter Q
- Player's input: key pair$(\mathsf{pk}, \mathsf{sk})$,
- i-th dealers' input: public key pk, $m_i \in [0,1]$, $y_i \in \mathcal{Y}$
- Player's output: $\hat{y}$
- Dealers' output: none

1. Initialize: Round $k = 1$.
2. The player chooses $j_k \in_r \{1, 2, ..., N\}$ and sends $\mathrm{Enc}_{\mathsf{pk}}(-j)$ to all dealers
3. For $i = 1, ..., N$,
   (a) The i-th dealer independently chooses $r_{i,k} \in_r \mathbb{Z}_Q$ and

$$a_{i,k} \leftarrow \begin{cases} j'_k, & \text{with prob. } m_i, \\ Y+1, & \text{otherwise.} \end{cases}$$

   where $j' \in_r \{1, 2, ..., N\}$. Then,

$$c_{i,k} \leftarrow \left(\mathrm{Enc}_{\mathsf{pk}}(a_{i,k}) \cdot \mathrm{Enc}_{\mathsf{pk}}(-j_k)\right)^{r_{i,k}} \cdot \mathrm{Enc}_{\mathsf{pk}}(y_i)$$

   and sends $c_{i,k}$ to the first dealer.
4. The first dealer randomly shuffles $(c_{k,1}, ..., c_{k,N})$ and sends them to the player
5. The player decrypts $u_i \leftarrow \mathrm{Dec}_{\mathsf{sk}}(c_{i,k})$ for all i and compute $Y' = \{u_1, ..., u_N\} \cap Y$.
   (a) If $Y' \neq \emptyset$, return $u \in_r Y'$ as $\hat{y}$.
   (b) Else, $k \leftarrow k+1$ and go to step 2.

図 2: Oblivious Roulette

このプロトコルの肝は, 暗号化された $a_{i,k}$ の計算法にある. $a_{i,k}$ は以下のような性質をもつよう設計されている

1. $a_{i,k}$ はプレイヤーのみが複号可能である
2. ディーラーが確率 m_i で有効なラベルを選択したときのみ, $a_{i,k}$ には意味のある値の暗号文が代入される
3. プレイヤーが $a_{1,k}, ..., a_{N,k}$ を複号化したとき, このうち一つだけ正しく複号できる
4. 各ディーラーによって生成された $a_{i,k}$ は, ランダムシャッフルした上でプレイヤーに渡され, プレイヤーは各値がどのディーラーから送られたか追跡できない

これらの 1-3 の性質により, 分散ルーレットの問題点であったプレイヤーによる $a_{j,k}$ の系列からの m_i の推測が防げ, 4 の性質よりプレイヤーによる $\hat{y}$ の発信元の特定を防ぐことができる. プロトコルの動作詳細については [5] もあわせて参照されたい.

続いて, 紛失ルーレットプロトコルのセキュリティを証明する. ここではプレイヤーとディーラーの振る舞いは *semi-honest* であることを仮定する. semi-honest とは, 各パーティーは前もって定められたプロトコルから逸脱することなく振舞うが, 計算途中で得た情報を, 他のパーティーの情報を推測するために利用することを仮定するモデルである.

表 2: Computation time per step (second) and info. model. The results are the average of 100 iterations.

	model	$N=2$	$N=4$	$N=8$	$N=16$	$N=32$
EW	full	0.562×10^{-8}	1.09×10^{-8}	2.03×10^{-8}	3.78×10^{-8}	7.25×10^{-8}
Exp3	partial	0.534×10^{-8}	1.02×10^{-8}	1.56×10^{-8}	2.75×10^{-8}	5.13×10^{-8}
SEW/OR	private	13.8	27.9	56.4	113	233

Lemma 3. プレイヤーとディーラーが *semi-honest* に振舞うならば, 紛失ルーレットプロトコルは *Statement 2* の意味で安全である. *(*証明略*)*

こちらも詳細は省略するが, 準同形性公開鍵暗号の利用と, 乱数の利用により, プロトコルの出力以外の値はすべて (たとえ復号鍵をもつプレイヤーにとっても) ランダムに分布するようプロトコルは設計されている.

5.2 Secure Exponential Weighting

最後に, プライベート情報モデルにおける secure exponential weighting (SEW) 法を示す. 基本的に完全情報モデルの exponential weighting 法に従うが以下の違いがある.

- $i=1,...,N$ において, i 番目のエキスパートは step 3 の式 2 による更新をを学習者の代わりに実行する
- 紛失ルーレットを予測 $\hat{y}_t = y_{j,t}$ を得るために用いる

Theorem 1. *Secure exponential weighting* 法は *Statement 1* の意味で安全である. *(*証明略*)*

secure exponential weighting 法におけるメッセージの交換はルーレットプロトコルにおいてのみ発生するため, 紛失ルーレットの安全性より, Theorem 1 も自明に成立する. 紛失ルーレットが用いられた場合は, 学習者の戦略は Lemma 2 に示すように $M(i;\boldsymbol{p})$ からわずかに逸脱するため, regret の上界は完全情報モデルにおける上界に比べわずかに変化する. 以下に secure exponential weighting の regret の上界を導く.

Theorem 2. 紛失ルーレットプロトコルを *secure exponential weighting* 法において用いるとき, *regret* の上界は以下で与えられる.

$$R_{\mathsf{SEW/OR},T} \le \frac{1-\gamma}{\eta}\ln N + \frac{\eta}{2}L_{\mathsf{SEW/OR}} + \frac{\gamma}{N}\sum_{i=1}^{N} L_i.$$

また $\gamma \le 1/T$ を仮定し, $\eta = \sqrt{2\ln N/T}$ とすれば $R_{\mathsf{SEW/OR},T} \le \sqrt{2T\ln N} + c$ である. ただし c は $c \in O(1)$ なる定数である. *(*証明略*)*

γ は鍵長 Q が大きい場合ほぼゼロに近い値をとるため, 紛失ルーレットプロトコルを用いた場合も, regret の上界は exponential weighting 法によるものと同一と考えてよい.

6. 実験と議論

提案プロトコルの効率性を評価する実験を行った. 問題設定は以下のとおりである. 環境は $y_t = \{0,1\}$ と各時刻にランダムに決定し, エキスパートおよび学習者はこれを各時刻で予測する. エキスパートは, 各エキスパートの正解率が $[0.5, 0.75]$ に一様に分布するよう生成し, そのうち一つのエキスパートの正解率は 0.75 とした. エキスパート数は $N=2,4,...,32$ とした. ステップあたりの regret を, 完全情報モデルにおける exponential weighting (EW), 部分情報モデルにおける Exp3, プライベート情報モデルにおける secure exponential weighting (SEW/OR) と比較した.

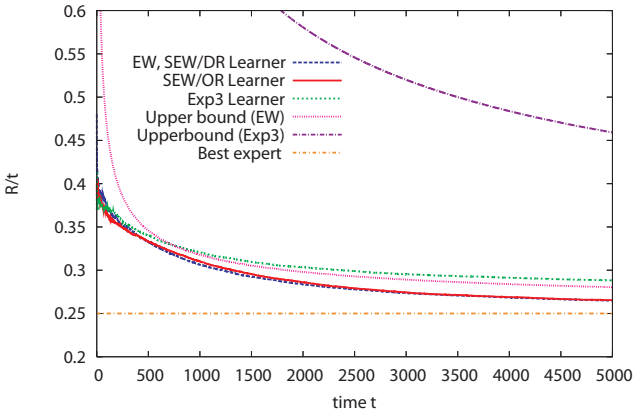

図 3: Expectation of regret per time (avg. of 100 iterations, $N=10$, $T=5000$).

図 3 はステップ数に対する各学習者の regret の時間平均を表している. SEW/OR の regret は定理が予測するように, EW ととほ同一である. プライベート情報モデルにおける SEW による学習者が, 部分情報モデルにおける学習者よりも少ない regret を実現していることに注目されたい. これは Exp3 による学習者は開示されていない情報を予測に利用しない反面, SEW による学習者は開示されていない情報も予測に利用しているためである.

表 2 は, オンライン予測におけるステップ毎の学習者の計算時間を表している. SEW の計算時間は EW や Exp3 に比べ非常に大きい. これはプロトコルに含まれる暗号部分の計算のためである. ただし 1 ラウンドあたりの SEW/OR の計算時間はこの設定では高々2-3 分であり, 意思決定感覚が 2-3 分よりも長い場合には, SEW は十分に実用的であると結論できる.

参考文献

[1] P. Auer, N. Cesa-Bianchi, Y. Freund, and R.E. Schapire. The nonstochastic multiarmed bandit problem. *SIAM Journal on Computing*, 32(1):48–77, 2003.

[2] A. Blum and Y. Mansour. Learning, regret minimization, and equilibria. *Algorithmic Game Theory*, pages 79–102, 2007.

[3] N. Littlestone and M.K. Warmuth. The weighted majority algorithm. *Information and computation*, 108:212–212, 1994.

[4] P. Paillier. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In *Eurocrypt'99*, pages 223–238. Springer, 1999.

[5] J. Sakuma and H. Arai. Online Prediction with Privacy. In *27th International Conference on Machine Learning, to appear*, 2010.