T-79.514 Special Course on Cryptology / Privacy-Preserving Data Mining

Comments on "Cryptographic Techniques for Privacy-Preserving Data Mining"

Johan Wallén

September 24, 2003

1 Introduction

In these notes, we briefly review the survey [3] on cryptographic techniques for privacy preserving data mining based on [2, 1]. The survey describes some cryptographic tools (oblivious transfer, oblivious polynomial evaluation and Yao's circuit evaluation protocol) and how they can be used to construct a privacy-preserving protocol for the ID3 algorithm for building decision trees. This protocol allows two parties owning confidential databases to run the ID3 algorithm on the union of their databases without revealing any unnecessary information to the other party. The core of the ID3 protocol is based on a protocol for computing shares of $x \ln x$ from shares of x.

In general, the survey gives a good and intuitive overview of the ID3 protocol and the underlying cryptographic building blocks. The level of of detail is suitable, and no special background in cryptography or data mining is needed to understand the presentation.

2 More detailed comments

Section 1 (Introduction: the setting) It would be nice with some example application of the ID3 protocol, where it is reasonable to assume that the parties are semi-honest (maybe from medical research?). Note also that semi-honest parties can be used to model attacks that take place after the protocol has been finished—for example, when the attacker breaks into one of the parties' computer and obtains a trace of the protocol run.

Section 2 (Introduction: cryptographic results) It would be good to start a new subsection when Yao's circuit evaluation protocol is described, since it is not directly related to oblivious polynomial evaluation.

The example base $\mathcal{B}$ should probably consist of all functions $g\colon \{0,1\}^2 \to \{0,1\}$ (and not $g\colon \{0,1\} \to \{0,1\}$).

Note that the two random values (W_i^0, W_i^1) of wire i should correspond in a random way to the values 0 and 1 (that is, W_i^b does not necessarily correspond to the value b). Otherwise, the second party learns the actual values of internal wires.

The construction of the garbled or encrypted circuit is probably the most difficult part to understand in the protocol. It might thus be good with a more precise description of how the tables T_g are constructed. One possible construction is as follows. Let F be a publicly known keyed pseudorandom function with key length n and output length $n+1$. For each wire, choose uniformly at random $r_0, r_1 \in \{0,1\}^n$ and $b \in \{0,1\}$. The encrypted signal corresponding to 0 is (r_0, b) and the encrypted signal corresponding to 1 is $(r_1, b \oplus 1)$. Consider a gate $g\colon \{0,1\}^2 \to \{0,1\}$ in the circuit. Let the encrypted input signals be (r_0, a), $(r_1, a \oplus 1)$, (s_0, b) and $(s_1, b \oplus 1)$, and let the encrypted output signals be (t_0, c) and $(t_1, c \oplus 1)$, where (r_0, a), (s_0, b) and (t_0, c) corresponds to the value 0. The table T_g holds four entries $T_g[0,0]$, $\ldots$, $T_g[1,1]$. If $g(\alpha, \beta) = \gamma$, the corresponding entry in the table is given by

$$T_g[x, y] = F_{r_\alpha}(x) \oplus F_{s_\beta}(y) \oplus (t_\gamma, z) \ ,$$

where $x = \alpha \oplus a$, $y = \beta \oplus b$ and $z = \gamma \oplus c$. The encrypted circuit consists of all the tables T_g. Party

A sends the encrypted circuit, the encrypted signal corresponding to its inputs and the correspondence between the encrypted signals and real values of the output wires to B. If party B knows the encrypted input signals (r, a) and (s, b) for a gate g, the encrypted output signal can be computed as

$$(t, c) = T_g[a, b] \oplus F_r(a) \oplus F_s(b) \ .$$

It should probably be mentioned that the oblivious transfers can be run in parallel. Thus, the protocol has a constant number of rounds.

Section 3 (Introduction: ID3 algorithm) It might be good to make it clearer that ID3 is easy to distribute given a protocol for finding the best attribute (that is, something along the lines of the discussion in [1, Section 5.1]) .

Section 5 (Finding the attribute with maximal gain: part one) The notation $T(a_j, c_i)$ is not defined (but its meaning is pretty obvious given the definition of $T(a_j)$).

Section 6 (Computing $x \ln x$) It would be nice to mention that $(v_1+v_2)\ln(v_1+v_2)$ is rounded to an integer. Otherwise, the expression $(v_1 + v_2)\ln(v_1 + v_2) \bmod |\mathcal{F}|$ looks confusing (first paragraph of Section 6).

The second paragraph of Section 6 is a bit confusing. It would probably be better just to say that the multiplication circuit is quadratic in the input size.

There seems to be a sign error in Section 6.2. Bob's share should probably be $P_1(u_2) + P_2(v_2) + u_2v_2 = \cdots = (v_1+v_2)(u_1+u_2) - v_1u_1 + r_1 + r_2$ and Alice's $v_1u_1 - r_1 - r_2$.

Typos Yehuda Lindell's name is misspelt in the abstract.

References

[1] Yehuda Lindell and Benny Pinkas. Privacy preserving data mining. *Journal of Cryptology*, 15(3):177–206, 2002. Earlier version presented at Crypto 2000.

[2] Benny Pinkas. Cryptographic techniques for privacy-preserving data mining. *ACM SIGKDD Explorations*, 4(2):12–19, 2003.

[3] Alexey Vyskubov. Cryptographic techniques for privacy-preserving data mining. Survey for the seminar T-79.514: Special Course on Cryptology / Privacy Preserving Data Mining at HUT, 23 September 2003.