УДК 004.056.5

КЛАССИФИКАЦИЯ ТИПА СХЕМЫ В ПРОТОКОЛАХ ДВУСТОРОННИХ ВЫЧИСЛЕНИЙ НА ОСНОВЕ АНАЛИЗА ТРАНСКРИПТА

Д.А. Руденок, У.А. Змачинская

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В работе исследуется определение типа логической схемы в протоколах 2PC (гарблированные схемы Яо) по транскрипту. На основе оптимизаций free-XOR и point-and-permute определены характерные размеры пакетов и задержки для гейтов AND и XOR. Сгенерированы транскрипты четырех реальных схем (mult2_64, AES-128,

SHA-256, FP-mul) с высоким уровнем шума и вариативности. Классификаторы Random Forest, логистическая регрессия и SVM достигли точности 99,9%. Это свидетельствует о существенной утечке информации о структуре функции, подтверждая необходимость разработки Function-Hiding MPC, скрывающей не только данные, но и логику вычислений.
Ключевые слова: гарблированные схемы Яо; безопасные двусторонние вычисления; классификация транскрипта; машинное обучение.

CLASSIFICATION OF CIRCUIT TYPE IN TWO-PARTY COMPUTATION PROTOCOLS BASED ON TRANSCRIPT ANALYSIS

D. Rudenok, U. Zmachynskaya
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. This study examines determining circuit type in Yao's 2PC protocols from transcripts. Based on free-XOR and point-and-permute optimizations, characteristic packet sizes and delays for AND and XOR gates were determined. Transcripts of four real circuits (mult2_64, AES-128, SHA-256, FP-mul) were generated with high noise and variability. Random Forest, logistic regression, and SVM classifiers achieved 99,9% accuracy. This indicates significant leakage of function structure, confirming the need for Function-Hiding MPC that conceals both data and computation logic.
Keywords: Yao's garbled circuits; secure two-party computation; transcript classification; machine learning.

Введение

Современные протоколы безопасных двусторонних вычислений (2PC) позволяют двум сторонам совместно вычислить функцию от их приватных входов, не раскрывая сами входы друг другу. Фундаментальная конструкция – гарблированные схемы Яо [1] – обеспечивает безопасность в модели получестного противника. Однако в реальных приложениях функция также может быть конфиденциальной (например, формула кредитного скоринга или диагностический алгоритм). Это привело к развитию направления Function-Hiding MPC (FH-MPC), где скрывается не только вход, но и сама вычисляемая функция [2].

Однако протоколы могут оставлять побочные следы (размеры пакетов, задержки), зависящие от структуры схемы (числа AND/XOR гейтов). Эти следы могут быть использованы для определения типа функции. В данной работе исследуется классификация типа схемы (AND или XOR) по статистическим признакам транскрипта.

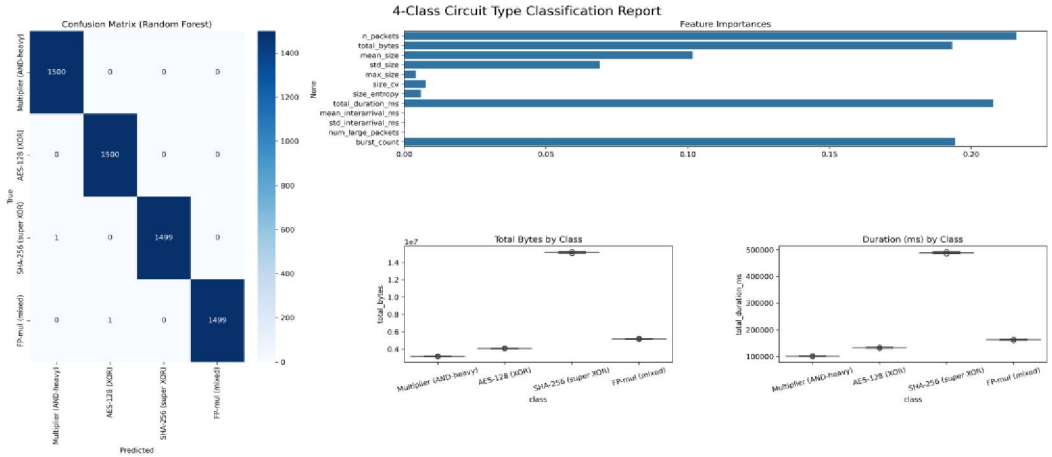
Основная часть

В данной работе рассматривается классический протокол Яо с оптимизаци-ями free-XOR и point-and-permute [3]. Гарблер строит булеву схему из гейтов AND и XOR. XOR не требуют передачи таблиц и обрабатываются быстро, каж-дый AND порождает 4 зашифрованных записи (16 байт) [4], что увеличивает трафик и время выполнения. Противник может извлечь из транскрипта призна-ки, коррелирующие с типом схемы.

Размеры пакетов и задержки выбраны на основе характеристик гарблиро-ванных схем. Для AND задан диапазон 60–68 байт (4 записи с заголовками), для XOR – 14–18 байт (служебный трафик) [3,5]. Временные задержки основаны на [1]: обработка AND занимает 4 мкс, XOR – практически мгновенно; в модели средняя задержка AND 0.15 мс, XOR 0.10 мс, отражая соотношение сложности и сетевые вариации.

Вместо двух классов с искусственными вероятностями использованы четыре реальные схемы из бенчмарков Bristol Fashion: mult2_64 (AND-богатая), AES-128, SHA-256 (XOR-богатые) и FP-mul (смешанная). Длина схем варьируется от сотен до тысяч гейтов. Транскрипты сгенерированы с высоким шумом (20% случайных замен гейтов), вариативностью размеров и задержек, добавлением служебных пакетов и WAN-задержек. Сгенерировано по 1500 примеров на класс. Из каждого транскрипта извлекались: количество пакетов, суммарный объем данных, статистики размеров и интервалов, энтропия, длительность.

Применены Random Forest, логистическая регрессия и SVM с RBF-ядром.



Матрица ошибок классификации четырех типов схем (Random Forest). Классы: 0 – mult2_64, 1 – AES-128, 2 – SHA-256, 3 – FP-mul

Confusion matrix of four circuit types (Random Forest). Classes: 0 – mult2_64, 1 – AES-128, 2 – SHA-256, 3 – FP-mul

Заключение

Эксперимент показал: на четырех реальных схемах (mult2_64, AES-128, SHA-256, FP-mul) все модели (Random Forest, логистическая регрессия, SVM) достигли точности 99,9%. Наибольший вклад в предсказания Random Forest внесли средний размер пакета, длительность и объем данных. Результаты демонстрируют утечку информации о структуре схемы через транскрипт, обосно-вывая необходимость создания механизмов защиты Function-Hiding MPC.

Список использованных источников

1. Wang X., Malozemoff A. J., Katz J. (2016) Faster two-party computation secure against malicious adversaries in the single-execution setting. *Cryptology ePrint Archive*, 3–5.

2. Yao A. C. (1982) Protocols for secure computations. *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*. 160–164.

3. Kolesnikov V., Schneider T. (2008) Improved garbled circuit: Free XOR gates and applications. *International Colloquium on Automata, Languages, and Programming*. 486–498.

4. Zahur S., Rosulek M., Evans D. (2015) Two halves make a whole. Advances in Cryptology *EUROCRYPT*. 220–250.

5 Rosulek M., Roy L. (2021) Three halves make a whole? Beating the half-gates lower bound for garbled circuits. *Advances in Cryptology – CRYPTO*. 2021. 3–32.

References

1. Wang X., Malozemoff A. J., Katz J. (2016) Faster two-party computation secure against malicious adversaries in the single-execution setting. *Cryptology ePrint Archive*, 3–5.

2. Yao A. C. (1982) Protocols for secure computations. *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*. 160–164.

3. Kolesnikov V., Schneider T. (2008) Improved garbled circuit: Free XOR gates and applications. *International Colloquium on Automata, Languages, and Programming*. 486–498.

4. Zahur S., Rosulek M., Evans D. (2015) Two halves make a whole. Advances in Cryptology *EUROCRYPT*. 220–250.

5 Rosulek M., Roy L. (2021) Three halves make a whole? Beating the half-gates lower bound for garbled circuits. *Advances in Cryptology – CRYPTO*. 2021. 3–32.

Сведения об авторах

Змачинская У.А., студент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», u.grazhdano4ka@gmail.com.

Руденок Д.А., студент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», diorud92@yahoo.com.

Information about the authors

Zmachynskaya U., student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", u.grazhdano4ka@gmail.com.

Rudenok D., student, *Educational Institution "Belarusian State University of Informatics and Radioelectronics",* diorud92@yahoo.com.