Realizing private and practical pharmacological collaboration

Brian Hie1, Hyunghoon Cho1, Bonnie Berger1,2†

Although combining data from multiple entities could power life-saving breakthroughs, open sharing of pharmacological data is generally not viable because of data privacy and intellectual property concerns. To this end, we leverage modern cryptographic tools to introduce a computational protocol for securely training a predictive model of drug–target interactions (DTIs) on a pooled dataset that overcomes barriers to data sharing by provably ensuring the confidentiality of all underlying drugs, targets, and observed interactions. Our protocol runs within days on a real dataset of more than 1 million interactions and is more accurate than state-of-the-art DTI prediction methods. Using our protocol, we discover previously unidentified DTIs that we experimentally validated via targeted assays. Our work lays a foundation for more effective and cooperative biomedical research.
complexity in the number of drugs and targets. In contrast, matrix factorization without side information (MF) lends itself to efficient MPC (23) but at the cost of greatly diminished model performance (Fig. 2, A and B, and fig. S1).

We next set out to demonstrate the scalability and predictive performance of Secure DTI on a much larger dataset that more accurately represents the scale of cross-institutional collaboration. We obtained 969,817 interactions from the STITCH 5 human dataset (24), which is, to our knowledge, the largest publicly available DTI dataset, and evaluated the cross-validation performance of Secure DTI. Even on the challenging task of predicting DTIs of previously unseen compounds, Secure DTI achieved high accuracy [area under the precision-recall curve (AUPR) of 0.95], which substantially outperforms matrix factorization methods (AUPRs of 0.50 and 0.43) (Fig. 2B and fig. S2). Owing to their quadratic scalability, other baseline methods could not be reasonably applied to a dataset of this size (even in plaintext). In contrast, Secure DTI took less than 4 days to train on millions of interactions over a WAN (materials and methods) and efficiently scaled with a linear dependence on the number of interactions in the dataset (Fig. 2C and table S1). Even when training Secure DTI on 2 million interactions, we extrapolate the total runtime for one epoch (one linear pass over the full, shuffled training set) to be ~2.2 days. In practice, we expect our model to achieve high accuracy in only a few training epochs; we obtained all of our reported results after 1.5 epochs. Additionally, given that our protocol admits flexibility in the choice of predictive model, we also securely trained a

Fig. 1. Secure pipeline for pharmacological collaboration. Collaborating entities (e.g., pharmaceutical companies or research laboratories) have large private datasets of DTIs, as well as corresponding chemical structures and protein sequences. In our protocol, the entities first use secret sharing to pool their data in a way that reveals no information about the underlying drugs, targets, or interactions (step 1). The collaborating entities then jointly execute a cryptographic protocol that trains a predictive model (e.g., a neural network) on the pooled dataset (step 2). The final model can be made available to participating entities or may be used to distribute DTI predictions to participants in a way that encourages greater data sharing (step 3).

Fig. 2. Prediction of DTIs. (A) Predictions from the DrugBank 3.0 dataset. Bar height corresponds to mean AUPR (area under the precision-recall curve), and error bars indicate SD. We compared Secure DTI to the plaintext methods BLMNII (20), NetLapRLS (16), HNM (21), MF (13), CMF (14), and DTINet (15), as reported in Luo et al. (15), by means of 10-fold cross-validation on balanced training and test sets (materials and methods; see fig. S1 for other evaluation settings). (B) Predictions from the STITCH 5 dataset with more than 1 million drug–target pairs. Secure DTI is compared with matrix factorization with (CMF) and without (MF) side information (see fig. S2 for other evaluation settings). Solid lines, sampling negative examples randomly; dashed lines, sampling negative examples while matching the relative frequencies of drugs and targets to those in the positive examples, representing a more challenging test case. Reported AUPRs are for the solid curves. (C) Runtime of our training protocol, over a local area network (LAN), for different dataset sizes. Box height represents SD.
support vector machine (SVM) instead of a neural network; the SVM reduced predictive performance (fig. S2).

To go beyond cross-validation and demonstrate the potential for novel discoveries that can result from our collaborative pipeline, we trained Secure DTI on all STITCH 5 interactions and scored the remaining possible drug–target pairs for interactivity, which is closer to how our pipeline would be used in a real-world setting. We controlled for bias toward highly represented drugs and targets in the dataset by either (i) filtering out any prediction involving both a drug and target highly represented in the original dataset (Secure DTI-A) or (ii) sampling negative examples (i.e., noninteractions) during model training such that each drug or target was seen at the same relative frequency in the negative examples as in the positive examples (Secure DTI-B). In both cases, many of our top predictions (5 of 12 for Secure DTI-A and 9 of 12 for Secure DTI-B) were validated by our own targeted assay experiments or by published experimental studies that have not yet been deposited into the STITCH database (Table 1). Our validation experiments suggest a previously unknown interaction between imatinib and ErbB4, for which we could not find any existing experimental support. It will be interesting to find out whether this interaction is confirmed by other studies. The top prediction from both methods was an interaction between the estrogen receptor (ER) and droloxifene, which had reached phase 3 clinical trials as an ER modulator for advanced breast cancer (25). Similarly, the predicted interaction between the vitamin D receptor (VDR) and seocalcitol has been clinically well established (26). Furthermore, some predictions without direct activity have strong evidence for an indirect functional interaction; for example, nutlin-3 has been shown to inhibit poly(ADP-ribose) polymerase 1 (PARP1) protein levels through p53-dependent proteasomal degradation in mouse fibroblasts (27). All of our findings were obtained without revealing any information about the underlyings drugs, targets, and interactions during the computation.

To provide enhanced interpretability of our reported results, we incorporated an additional step into our pipeline for securely evaluating the impact of individual input features on the prediction outcome (supplementary text). When applied to our top predictions from the STITCH database, this capability linked drugs to specific ligand-binding or functional sites within the predicted target (table S3).

Table 1. Predicted out-of-dataset DTIs. We trained Secure DTI on all human DTIs from STITCH 5, which we used to score and rank all pairs of drugs and targets that are not in the STITCH database. We implemented two methods to control for model bias toward overrepresented drugs and targets, either (i) filtering out predictions involving a drug and target that are both highly represented in STITCH (Secure DTI-A) or (ii) retraining Secure DTI such that the negative training examples had an equal representation of drugs and targets compared with the positive training examples (Secure DTI-B) (materials and methods). Interactions labeled N/A involve commercially unavailable compounds and thus could not be tested. “Active” interactions have median inhibitory concentrations <100 μM, whereas “inconclusive” interactions demonstrate observable activity only at one or two high-concentration levels, a potential artifact of compound aggregation. We labeled the interaction between actinomycin D and PARP1 as “weakly active” because consistent activity was observed over a wide range of concentrations, including near-50% inhibition at 100 μM (our highest tested concentration). However, it should be noted that its dose-response curve does not follow a typical sigmoidal shape. References and additional information are provided in table S2.

| Rank | Drug    | Target | Experimental validation | Drug    | Target | Experimental validation |
|------|---------|--------|-------------------------|---------|--------|-------------------------|
| 1    | Droloxifene | ERα    | Active* | Droloxifene | ERβ    | Active* |
| 2    | Droloxifene | ERβ    | Active* | CHEMBL601690 | p110α  | Active |
| 3    | Imatinib   | ErbB3  | Inconclusive* | Droloxifene | ERα    | Active* |
| 4    | Imatinib   | ErbB4  | Active* | Seocalcitol | VDR   | Active |
| 5    | Nutlin-3   | PARP1  | Inactive* | AGN-PC-0A9TBG | PPARy  | Active |
| 6    | Droloxifene | PgR    | Inactive* | CHEMBL589864 | p110α  | Active |
| 7    | Actinomycin D | PARP1 | Weakly active* | T5958429 | PARP1  | Active |
| 8    | Hoechst 33258 | PARP1 | Inactive* | AGN-PC-0N7PYE | Factor Xα | Active |
| 9    | GW-501516  | GR     | Inactive* | AGN-PC-00D30 | PPARy  | Active |
| 10   | AGN-PC-0BFP0W | Lck    | Active | AGN-PC-0NABN | PTPZR21 | N/A |
| 11   | CHEMBL2332055 | mGluR1 | Inconclusive* | AGN-PC-0NABN | PTPRG  | N/A |
| 12   | CHEMBL2332055 | mGluR5 | Inconclusive* | AGN-PC-088DZ9 | PROC   | N/A |

*Predicted interactions, including all testable interactions without existing literature support, that were experimentally validated in our study.
information leakage, a technique known as differential privacy (29, 30), a method being developed for differentially private neural networks can be used in conjunction with our protocol (37). An alternative strategy for collaborative neural network-based prediction is to train local models in plaintext and use secure protocols only when periodically averaging over these models, thus minimizing the amount of cryptographic overhead (32, 33). However, this approach is vulnerable to reverse engineering–based attacks in which a malicious collaborator jointly trains a local model (e.g., a generative adversarial network) that uncovers information about private data owned by honest collaborators, even when differential privacy techniques are applied (34). In contrast, securely training a single model over a decentralized network of computing parties, as in our pipeline, is not vulnerable to such attacks.

Our privacy-preserving protocols generalize to other large-scale data sharing problems beyond drug discovery, with the highest potential for impact in areas that suffer from a lack of collaboration due to privacy concerns, such as predictive analyses of electronic health records. Our practical demonstration of secure, large-scale machine learning with neural networks may also provide a useful blueprint for enhancing privacy in many other domains where neural networks have been shown to be successful.

REFERENCES AND NOTES
1. S. Reardon, Nature 10.1038/nature.2014.14672 (2014).
2. J. Levy, The age of collaboration: why pharma companies now have to work together, Pharmalive (2015); www.pharmalive.com/news/501725/age-collaboration-why-pharma-companies-now-have-work-together.
3. M. Wilhelm, Big Pharma Buys Into Crowdsourcing for Drug Discovery, Wired (2017); www.wired.com/story/big-pharma-buys-into-crowdsourcing-for-drug-discovery/.
4. J. Hunter, Collaboration for innovation is the new mantra for the pharmaceutical industry. Drug Discovery World (2014); www.ddw-online.com/business/pl217613-collaboration-for-innovation-is-the-new-mantra-for-the-pharmaceutical-industry-spring-14.html.
5. Johnson & Johnson Innovation Announces New Collaborations Advancing Ground-Breaking Biomedical Innovation Around the Globe,” press release; www.njinnovation.com/sites/default/files/jj_bio_2017_press_release_06-15-17.pdf.
6. I. Khurana, Drug Discov. Today 17, 1088–1102 (2012).
7. D. Cressey, Nature 471, 17–18 (2011).
8. S. M. Paul et al., Nat. Rev. Drug Discov. 9, 203–214 (2010).
9. R. Cramer, I. B. Damgård, J. B. Nielsen, Secure Multiparty Computation and Secret Sharing (Cambridge Univ. Press, ed. 1, 2015).
10. M. Ben-Or, S. Goldwasser, A. Wigderson, in Proceedings of the 20th Annual ACM Symposium on Theory of Computing (ACM, 1988), pp. 1–10.
11. D. Chebrolu, A. Sawicka, in Financial Cryptography and Data Security, R. Sion, Ed. (Lecture Notes in Computer Science Series, Springer, 2010), pp. 35–50.
12. H. Cho, D. Wu, B. Berger, Nat. Biotechnol. 36, 547–551 (2018).
13. M. C. Cobanoglu, C. Liu, F. Hu, Z. N. Othayi, I. Buhar, J. Chem. Inf. Model. 53, 3396–3409 (2013).
14. X. Zheng, H. Ding, H. Mamiishi, S. Zhu, in Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (2013), pp. 1025–1033.
15. Y. Liao et al., Nat. Commun. 8, 573 (2017).
16. Z. Xia, L. Y. Wu, X. Zhou, S. T. C. Wong, BMC Syst. Biol. 4 (suppl. 2), S6 (2010).
17. Y. LeCun, Y. Bengio, G. Hinton, Nature 521, 436–444 (2015).
18. X. Glorot, A. Bordes, Y. Bengio, in Proceedings of the 14th International Conference on Artificial Intelligence and Statistics, G. Gordon, D. Dunson, M. Dudik, Eds. (JMLR W&CP, 2011), vol. 15, pp. 315–323.
19. F. Mohassess, Y. Zhang, in Proceedings of the 2017 IEEE Symposium on Security and Privacy (IEEE, 2017), pp. 19–38.
20. J. P. Mei, C. K. Kwok, P. Yang, X. L. Li, J. Zheng, Bioinformatics 29, 238–248 (2013).
21. W. Wang, S. Yang, X. Zhang, J. Li, Bioinformatics 30, 2923–2930 (2014).
22. C. Knox et al., Nucleic Acids Res. 39 (suppl. 1), D1035–D1041 (2011).
23. V. Nikolaenko et al., in Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security (ACM, 2013), pp. 891–892.
24. D. Sklarczyk et al., Nucleic Acids Res. 44, D380–D384 (2016).
25. A. Buzdar et al., Breast Cancer Res. Treat. 73, 161–175 (2002).
26. G. Tocchini-Valentini, N. Rochel, J. M. Wurtz, D. Moras, J. Med. Chem. 47, 1956–1961 (2004).
27. S. Matsushima et al., Biochem. Biophys. Res. Commun. 407, 557–561 (2011).
28. I. D. DeLisi, S. P. Castro, N. Smart, S. Zakarias, in Advances in Cryptology – CRYPTO 2012, R. Safavi-Naini, R. Canetti, Eds. (Lecture Notes in Computer Series, Springer, 2012), vol. 7417, pp. 643–662.
29. C. Dwork, F. McSherry, K. Nissim, A. Smith, Theory Cryptogr. 295–294 (2006).
30. S. Simmons, C. Sahinalp, B. Berger, Cell Syst. 3, 54–61 (2016).
31. M. Abadi et al., in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (ACM, 2016), pp. 308–318.
32. K. Bonwitz et al., in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (ACM, 2017), pp. 1175–1191.
33. R. Shokri, V. Shmatikov, in 2015 53rd Annual Allerton Conference on Communication, Control, and Computing (IEEE, 2016), pp. 909–910.
34. B. Htaj, G. Cohen, Perez-Cruz, arXiv:1702.07464 [cs.CR] (24 February 2017).

ACKNOWLEDGMENTS
We thank E. Irvine and P. Macaluso for assistance with validation experiments. Funding: B.H. and H.C. are partially supported by NIH grant R01GM081871 (to B.B.). H.C. is also partially supported by the Kwanjeong Educational Foundation. Author contributions: B.H., H.C., and B.B. developed the computational methods. B.H. and H.C. implemented the protocol and performed the analyses. B.B. guided the research. All authors wrote the manuscript.

Competing interests: A provisional patent application on this work (serial no. 62/611,678) was filed on 29 December 2017. Data and materials availability: Code and data are available at http://secure-dti.csail.mit.edu. Drug-target interaction datasets were obtained from DrugBank version 3.0 (www.drugbank.ca/) and STITCH version 5.0 (http://stitch.embl.de/). Protein domain information is available from the Pfam database (https://pfam.xfam.org/).

SUPPLEMENTARY MATERIALS
www.sciencemag.org/content/362/6412/347/suppl/DC1 Materials and Methods Supplementary Text Figs. S1 to S4 Tables S1 to S3 References (25–58)
2 March 2018; accepted 28 August 2018 10.1126/science.aat4807