American Economic Review: Papers & Proceedings 2012, 102(3): 65–70
http://dx.doi.org/10.1257/aer.102.3.65

Privacy-Preserving Methods for Sharing Financial Risk Exposures[†]

By Emmanuel A. Abbe, Amir E. Khandani, and Andrew W. Lo*

While there is still considerable controversy over the root causes of the Financial Crisis of 2007–2009, there is little dispute that regulators, policymakers, and the financial industry did not have ready access to information with which early warning signals could have been generated. For example, prior to the Dodd-Frank Act of 2010, even systemically important financial institutions such as AIG and Lehman Brothers were not obligated to report their amount of financial leverage, asset illiquidity, counterparty risk exposures, market share, and other critical risk data to any regulatory agency. If aggregated over the entire financial industry, such data could have played a critical role in providing regulators and investors with advance notice of AIG's unusually concentrated position in credit default swaps, as well as the exposure of money market funds to Lehman bonds. Of course, such information is currently considered proprietary and highly confidential, and releasing it into the public domain would clearly disadvantage certain companies and benefit their competitors. But without this information, regulators and investors cannot react in a timely and measured fashion to growing threats to financial stability, thereby assuring their realization.

At the heart of this vexing challenge is privacy. Unlike other industries in which intellectual property is protected by patents, the financial industry consists primarily of "business processes" that the US Patent Office has deemed unpatentable, at least until recently. Therefore, trade secrecy has become the preferred method by which financial institutions protect the vast majority of their intellectual property, hence their need to limit disclosure of their business processes, methods, and data. Forcing a financial institution to publicly disclose its proprietary information—and without the quid pro quo of 17-year exclusivity that a patent affords—will obviously discourage innovation, which benefits no one. Accordingly, government policy has tread carefully on the financial industry's disclosure requirements.

In this paper, we propose a new approach to financial systemic risk management and monitoring via cryptographic computational methods in which the two seemingly irreconcilable objectives of protecting trade secrets and providing the public with systemic risk transparency can be achieved simultaneously. To accomplish these goals, we develop protocols for securely computing aggregate risk measures. The protocols are constructed using secure multiparty computation tools (Yao 1982; Goldreich, Micali, and Wigderson 1987; Ben-Or, Goldwasser, and Wigderson 1988; Chaum, Crépeau, and Damgard 1988; Beaver, Micali, and Rogaway 1990; Cramer et al. 1999), specifically using secret sharing (Shamir 1979). It is well known that general Boolean functions can be securely computed using "circuit evaluation protocols" (Goldreich, Micali, and Wigderson 1987;

*Abbe: EPFL School of Communication and Computer Sciences, INR130 Station 14, Lausanne 1015, Switzerland (e-mail: emmanuelabbe@gmail.com); Khandani: MIT Laboratory for Financial Engineering, 100 Main Street, Cambridge, MA 02142 (e-mail: khandani@mit.edu); Lo: MIT Sloan School of Management, Laboratory for Financial Engineering, CSAIL/EECS, and AlphaSimplex Group, 100 Main Street, Cambridge, MA 02142 (e-mail: alo@mit.edu). We thank Jayna Cummings, Arnout Eikeboom, Lars Hansen, Martin Hirt, Bryan Kelly, Bob Merton, Silvio Micali, and Ron Rivest for helpful comments and discussion. The views and opinions expressed in this article are those of the authors only, and do not necessarily represent the views and opinions of AlphaSimplex, EPFL, MIT, any of their affiliates or employees, or any of the individuals acknowledged above.

[†] To view additional materials, visit the article page at http://dx.doi.org/10.1257/aer.102.3.65.

Ben-Or, Goldwasser, and Wigderson 1988), and because computing any function on real-valued data is approximated arbitrarily well by computing a function on quantized (or binary) data, in principle such protocols can also be used for real-valued functions. For arbitrary functions and high precision, however, the resulting protocols may be computationally too demanding and therefore impractical.

We show that for computing aggregate risk measures based on standard sample moments such as means, variances, and covariances—the typical building blocks of financial risk measures (see for example, Bisias et al. 2012)—simple and efficient protocols can be developed. Using these methods, it is possible to compute the aggregate risk exposures of a group of financial institutions—for example, a concentration (or "Herfindahl") index of the credit default swaps market, the aggregate leverage of the hedge fund industry, or the margin-to-equity ratio of all futures brokers—without jeopardizing the privacy of any individual institution. More importantly, these protocols will enable regulators and the public to accurately measure and monitor the amount of risk in the financial system while preserving the intellectual property and privacy of individual financial institutions.

Privacy-preserving risk measures may also facilitate the ability of the financial industry to regulate itself more effectively. Despite the long history of "self-regulatory organizations" (SROs) in financial services, the efficacy of self-regulation has been sorely tested by the recent financial crisis. SROs may, however, be considerably more effective if they had access to timely and accurate information about systemic risk that did not place any single stakeholder at a competitive disadvantage. The broad dissemination of privacy-preserving systemic risk measures will enable the public to respond appropriately as well, reducing general risk-taking activity as the threat of losses looms larger due to increasing systemic exposures. Truly sustainable financial stability is more likely to be achieved by such self-correcting feedback loops than by any set of regulatory measures.

I. Secure Protocols

Several important statistical measures such as mean, standard deviation, concentration ratios, and pairwise correlations can be obtained by taking summations and inner products on the data. Therefore, we present secure protocols for these two specific functions. In particular, we assume that the parties follow the protocol requirements (although they may be curious[1] and try to learn additional information through the protocol) and show that the specified protocols afford real precision while being efficient with respect to computations and communication rounds. It would also be interesting to investigate secure protocols for more general systemic risk measures or adversarial models, and some extensions are briefly discussed in this paper but left for future research.

We start with a basic protocol to securely compute the sum of m secret numbers when the parties are honest but curious (i.e., they do not deviate from the protocol although they may collect the data exchanged in the protocol and try to learn more information about other parties' data). We assume that each number belongs to a known range, which we pick to be $[0, 1)$ for simplicity. Recall that the operation a modulo m (written a mod m) produces the unique number $a + km \in [0, m)$ where k is an integer; e.g., $3.6 \bmod 2 = 1.6$.

A. *Secure-Sum Protocol*

For $i = 1, \ldots, m$, each party i privately owns the number $x_i \in [0, 1)$ as an input. The protocol outputs a number S to each party, which is equal to the real sum $s = \sum_{i=1}^{m} x_i$, if parties follow the protocol correctly.

Secure-Sum Protocol:

(i) For each i, j with $i \neq j$, party i provides privately to party j a number R_{ij} drawn uniformly at random in $[0, m)$.

(ii) For each i, party i adds to its secret number the numbers it has received from other parties and subtracts the numbers it has provided to other parties. Formally, party i computes $S_i = x_i + \sum_{\substack{j \in \{1, \ldots, m\} \\ j \neq i}} R_{ji} - \sum_{\substack{j \in \{1, \ldots, m\} \\ j \neq i}} R_{ij} \bmod m.$

[1] Formally, we assume "honest but curious" parties (Goldreich 1998).

Party i reveals S_i to the other parties.

(iii) Each party computes $S = \sum_{i=1}^{m} S_i \bmod m$.

If the parties follow the protocol correctly, it is easy to check that $S = \sum_{i=1}^{m} x_i$ (i.e., the correct sum is always obtained), since each element R_{ij} is added and subtracted once in S. In addition, we show that this protocol reveals nothing else about the secret numbers than their sum, even if the parties attempt to infer more from the exchanged data. For example, Party 1 may try to learn more about other parties' secret numbers by using the information gathered in S_1, S_2, S_3. We provide a privacy guarantee in the following theorem, which is based on basic probability results (see Abbe, Khandani, and Lo 2011 for a proof, as well as a simple demonstration of this protocol).

THEOREM 1: *Let* $x_1, \ldots, x_m$ *be* m *privately owned real numbers in* $[0, 1)$. *Let* $i \in \{1, \ldots, m\}$ *and* View_i *denote the view of party* i *obtained from the Secure-Sum Protocol with inputs* $x_1, \ldots, x_m$, *assuming honest but curious parties. The protocol outputs the sum* $s = \sum_{i=1}^{m} x_i$ *and the distribution of* View_i *depends on* $x_1, \ldots, x_m$ *only through* s *and* x_i.

Theorem 1 ensures that the Secure-Sum Protocol outputs the sum of m privately owned real numbers and does not reveal any additional information about the individual numbers if parties do not deviate from the protocol. Extensions to malicious parties can also be considered but are not discussed here. In particular, the protocol is robust to collusion. Other variants of this protocol include exchanging fewer random numbers to minimize the communication between parties while preserving the privacy (but this may reduce the robustness to collusion), and exchanging additional numbers to check the correctness of the parties' computations. One may also use a "regulator party" who does not possess any inputs or learn additional information about other parties' inputs, but may improve the privacy or efficacy of the protocol.

B. *Secure-Inner-Product Protocol*

To compute securely the inner product of two real vectors, slightly more sophisticated protocols are developed and presented in Abbe, Khandani, and Lo (2011), using secret sharing (Shamir 1979; Ben-Or, Goldwasser, and Wigderson 1988; Chaum, Crépeau, and Damgard 1988) and Oblivious Transfer (Rabin 1981; Even, Goldreich, and Lempel 1985; Goldreich, Micali, and Wigderson 1987). The variants include information-theoretic and cryptographic protocols on quantized or real data, and have different attributes discussed in Abbe, Khandani, and Lo (2011). We present here the first protocol on quantized data, which uses a dummy party (helping with computations but not possessing inputs or receiving meaningful information).

Secure-Inner-Product Protocol.—Common inputs are $q \in \mathbb{Z}_+$ (the quantization level), $n \in \mathbb{Z}_+$ (the vector dimensions), and p a prime larger than $q^2 n$. Party 1 inputs: $x_1, \ldots, x_n \in \mathbb{Z}_q$. Party 2 inputs: $y_1, \ldots, y_n \in \mathbb{Z}_q$. Party 3 inputs: none. The protocol outputs a number R to parties 1 and 2, which is equal to the inner product $\rho = \sum_{i=1}^{n} x_i y_i$ if the parties follow the protocol correctly.

(i) For $i = 1, \ldots, n$, party 1 splits x_i in three shares $x_i(1)$, $x_i(2)$ and $x_i(3)$ uniformly drawn in $\sum_3(x_i, \mathbb{F}_p) := \{(a, b, c) \in \mathbb{F}_p^3 : a + b + c \bmod p = x_i\}$ and party 2 splits y_i in three shares $y_i(1)$, $y_i(2)$, and $y_i(3)$ uniformly drawn in $\sum_3(y_i, \mathbb{F}_p)$. Party 1 provides privately to party 2 the shares $x_i(1)$, $x_i(2)$, and privately to party 3 the share $x_i(3)$. Party 2 provides privately to party 1 the shares $y_i(1), y_i(2)$ and privately to party 3 the share $y_i(3)$.

(ii) Party 1 sets $p_i(1) = (x_i(1) + x_i(3))(y_i(1) + y_i(2)) \bmod p$ and $\rho(1) = \sum_{i=1}^{n} p_i(1) \bmod p$, party 2 sets $p_i(2) = (x_i(1) + x_i(2))y_i(3) + x_i(2)(y_i(1) + y_i(2)) \bmod p$ and $\rho(2) = \sum_{i=1}^{n} p_i(2) \bmod p$, and party 3 sets $p_i(3) = x_i(3)y_i(3) \bmod p$ and $\rho(3) = \sum_{i=1}^{n} p_i(3) \bmod p$. For $m = 1, 2, 3$, party m splits $\rho(m)$ in three shares $\rho(m, 1)$, $\rho(m, 2)$, and $\rho(m, 3)$ uniformly drawn in $\sum_3(\rho(m), \mathbb{F}_p)$ and reveals privately $\rho(m, k)$ to party k, for $k = 1, 2, 3$.

(iii) For $k = 1, 2, 3$, party k computes $R(k) = \sum_{m=1}^{3} \rho(m, k) \bmod p$. Parties 1 and 2 privately exchange $R(1)$ and $R(2)$

and party 3 provides $R(3)$ to parties 1 and 2. Parties 1 and 2 compute $R = R(1) + R(2) + R(3)$.

THEOREM 2: *Let* $x = [x_1, \dots, x_n]$ *and* $y = [y_1, \dots, y_n]$ *be two privately owned vectors on* $\mathbb{Z}_q^n$. *Let* View_1 *denote the view of party* 1 *obtained from the Secure-Inner-Product Protocol with inputs* x, y, *assuming honest but curious parties. The protocol outputs the inner product* $\rho = \sum_{i=1}^{n} x_i y_i$ *and the distribution of* View_1 *depends on* x, y *only through* ρ *and* x. *The reciprocal result holds for party* 2. *The distribution of the view of party* 3 *does not depend on* x, y.

This theorem ensures that the Secure-Inner-Product Protocol outputs the sum of two privately owned quantized vectors and does not reveal any additional information about the individual vectors if the parties do not deviate from the protocol. Abbe, Khandani, and Lo (2011) provide a simple numerical example of this algorithm, as well as a more detailed illustrative application using publicly available quarterly data from June 1986 to December 2010 (released in arrears by the US Federal Reserve) on the total amount of outstanding real estate–related loans issued by three major bank holding companies: Bank of America, JPMorgan, and Wells Fargo. Figure 1 displays the three time series of encrypted data (step 2 of the Secure-Sum Protocol above) revealed by each of the three institutions to each other. As is evident from visual inspection, the three encrypted series are random. They have a different scale than the original series and show no trend even though no clear trends exist in the unencrypted data.[2] Yet the sum of the three encrypted time series is identical to the sum of the unencrypted time series, which may be a useful aggregate measure of "crowdedness" and potential illiquidity in this market.

II. Discussion

By construction, privacy-preserving measures of financial risk exposures cannot be "reverse-engineered" to yield information about the individual constituents. Accordingly, there is no guarantee that the individual inputs are truthful. In this respect, the potential for misreporting and fraud are no different for these measures than they are for current reporting obligations by financial institutions to their regulators, and existing mechanisms for ensuring compliance—random periodic examinations and severe criminal and civil penalties for misleading disclosures—must be applied here as well. Of course, the algorithms proposed in this paper can be easily modified to produce a cryptographically secure audit trail that would enable the regulators to verify the historical truthfulness of the participants that are selected for random periodic audits.[3]

Unlike traditional regulatory disclosures, however, privacy-preserving measures will provide users with a strong incentive to be truthful because the mathematical guarantee of privacy eliminates the primary motivation for obfuscation. Since each institution's proprietary information remains private even after disclosure, dishonesty yields no discernible benefits but could have tremendous reputational costs, and this asymmetric payoff provides significantly greater economic incentive for compliance. Moreover, accurate and timely measures of system-wide risk exposures can benefit the entire industry in allowing institutions and investors to engage in self-correcting behavior that can reduce the likelihood of systemic shocks. For example, if all stakeholders were able to monitor the aggregate amount of leverage in the financial system at all times, there is a greater chance that market participants would become more wary and less aggressive as they observe leverage rising beyond prudent levels.

A related issue is whether participation in privacy-preserving disclosures of financial risk exposures is voluntary or mandated by regulation. Given the extremely low cost/benefit ratio of such disclosures, there is reason to believe that the financial industry may well adopt such disclosures voluntarily. A case in point is Markit,

[2] The scale of the encrypted data is controlled by the support of the distribution used for R_{ij} (parameter m in Step 1 of the Secure-sum protocol). For this example, we rounded the holding of each bank to the nearest billion dollars and set $m = 10{,}000$.

[3] In ongoing research, we take a more radical application of secure multiparty computation that is to include the regulator as one of the parties. This one simple change not only eliminates the need for a trusted party, but also shifts the role of human supervision from monitoring data to monitoring protocols, dramatically leveraging the scarcest resource of regulatory agencies.

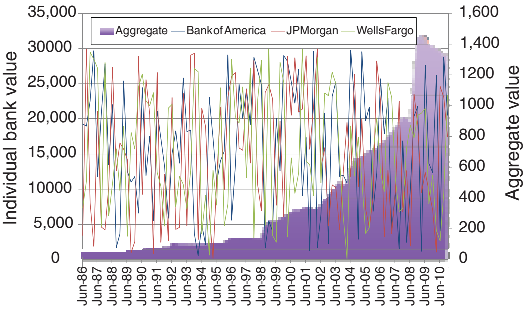

Figure 1. Historical Quarterly Time Series of Three Privacy-Preserving Measures of Total Real Estate Loans Outstanding of Bank of America, JPMorgan, and Wells Fargo from June 1986 to December 2010 (*for which the sum is identical to the sum of the unencrypted time series*)

a successful industry consortium of dealers of credit default swaps (CDS) that emerged in 2001 to pool confidential pricing data on individual CDS transactions and make the anonymized data available to each other and the public so as to promote transparency and liquidity in this market. According to Markit's website, the data of its consortium members are "... provided on equal terms to whoever wanted to use it, with the same data released to all customers at the same time, giving both the sell-side and buy-side access to exactly the same daily valuation and risk management information."[4] From this carefully crafted statement, it is clear that equitable and easy access to data is of paramount importance in structuring this popular data-sharing consortium. Privacy-preserving methods of sharing information could greatly enhance the efficacy and popularity of such cooperatives.

The same motivation applies to the sharing of aggregate financial risk exposures, but with even greater stakes as the recent financial crisis has demonstrated. Once a privacy-preserving system-risk-exposures consortium is established, the benefits will so clearly dominate the nominal costs of participation that it should gain widespread acceptance and adoption in short order. Indeed, participation in such a consortium may serve as a visible commitment to industry best practices that yields tangible benefits for business development, leading to a "virtuous cycle" of privacy-preserving risk disclosure throughout the financial industry.

III. Conclusion

Privacy-preserving measures of financial risk exposures solve the challenge of measuring aggregate risk among multiple financial institutions without encroaching on the privacy of any individual institution. Current approaches to addressing this challenge require trusted third parties, i.e., regulators, to collect, archive, and properly assess systemic risk. Apart from the burden this places on government oversight, such an approach is also highly inefficient, requiring properly targeted and perfectly timed regulatory intervention among an increasingly complex and dynamic financial system. Privacy-preserving measures can promote more efficient "crowdsourced" responses to emerging threats to systemic stability, enabling both regulators and market participants to accurately monitor systemic risks in a timely and coordinated fashion, creating a more responsive negative-feedback loop for stabilizing the financial system. This feature may be especially valuable for promoting international coordination among multiple regulatory jurisdictions. While a certain degree of regulatory competition is unavoidable given the competitive nature of sovereign governments, privacy-preserving measures do eliminate a significant political obstacle to regulatory collaboration across national boundaries.

Privacy-preserving risk measures have several other financial and nonfinancial applications. Investors such as endowments, foundations, pension and sovereign wealth funds can use these measures to ensure that their investments in various proprietary vehicles—hedge funds, private equity, and other private partnerships—are sufficiently diversified and not overly concentrated in a small number of risk factors. For example, the Secure-Inner-Product Protocol can be used to calculate correlations without requiring these private partnerships to share their actual returns with each other or even with the pension fund investor. Financial auditors charged with the task of valuing illiquid assets at a given financial institution can use these measures to compare and contrast their valuations with the industry average and the dispersion of valuations across multiple institutions. Real-time indexes of the

[4] http://www.markit.com/en/media-centre/about-markit-cds-pricing.page (acccessed February 29, 2012).

aggregate amount of hedging activity in systemically important markets like the S&P 500 futures contract may be constructed, which could have served as an early warning signal for the "Flash Crash" of May 6, 2010.

More broadly, privacy-preserving measures of risk exposures may be useful in other industries in which aggregate risks are created by individual institutions and where maintaining privacy in computing such risks is important for promoting transparency and innovation, such as healthcare, epidemiology, and agribusiness.

REFERENCES

Abbe, Emmanuel, Amir Khandani, and Andrew W. Lo. 2011. "Privacy-Preserving Methods for Sharing Financial Risk Exposures." Unpublished.

Beaver, Donald, Silvio Micali, and Philip Rogaway. 1990. "The Round Complexity of Secure Protocols." In *Proceedings of the Twenty-Second Annual Association for Computing Machinery Symposium on Theory of Computing*, 503–13. New York: Association for Computing Machinery.

Ben-Or, Michael, Shafi Goldwasser, and Avi Wigderson. 1988. "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation." In *Proceedings of the Twentieth Annual Association for Computing Machinery Symposium on Theory of Computing*, 1–10. New York: Association for Computing Machinery.

Bisias, Dimitrios, Mark D. Flood, Andrew W. Lo, and Stavros Valavanis. 2012. "A Survey of Systemic Risk Analytics." US Department of Treasury Office of Financial Research Working Paper No. 0001.

Chaum, David, Claude Crépeau, and Ivan Damgard. 1988. "Multiparty unconditionally secure protocols." In *Proceedings of the Twentieth Annual Association for Computing Machinery Symposium on Theory of Computing*, 11–19. New York: Association for Computing Machinery.

Cramer, Ronald, Ivan Damgard, Stefan Dziembowski, Martin Hirt, and Tal Rabin. 1999. "Efficient Multiparty Computations With Dishonest Minority." *EuroCrypt* 311–26.

Even, Shimon, Oded Goldreich, and Abraham Lempel. 1985. "A Randomized Protocol for Signing Contracts." *Communications of the Association for Computing Machinery* 28 (6): 637–47.

Goldreich, Oded. 1998. "Secure Multi-Party Computation." Unpublished.

Goldreich, Oded, Silvio Micali, and Avi Wigderson. 1987. "How to Play Any Mental Game." In *Proceedings of the Nineteenth Annual Association for Computing Machinery Symposium on Theory of Computing,* 218–29. New York: Association for Computing Machinery.

Rabin, Michael O. 1981. "How to Exchange Secrets by Oblivious Transfer." Aiken Computation Laboratory Harvard University TR-81.

Shamir, Adi. 1979. "How to Share a Secret." *Communications of the Association for Computing Machinery* 22 (11): 612–13.

Yao, Andrew C. 1982. "Protocols for Secure Computations." In *Proceedings of the Twenty-Third Annual Association for Computing Machinery Symposium on Theory of Computing* 160–64.