安全多方计算

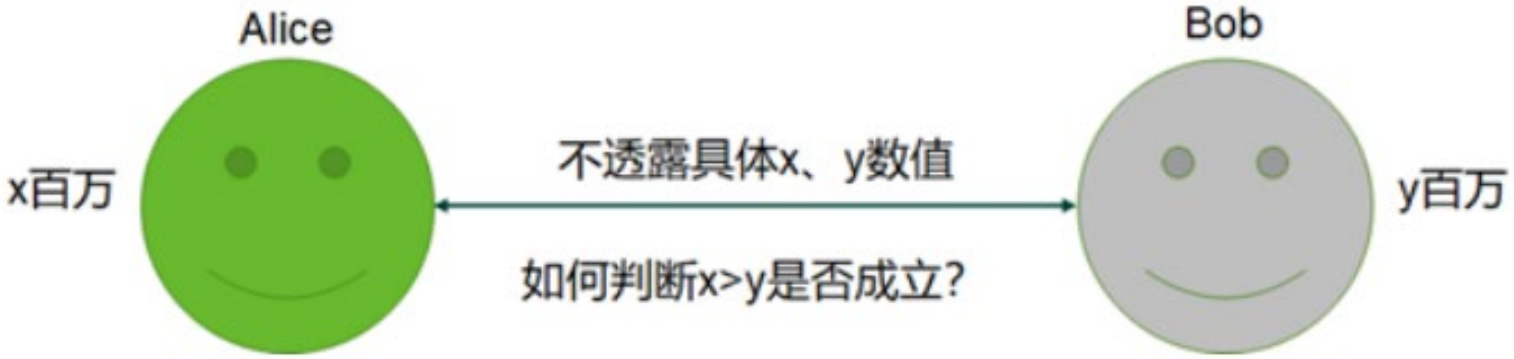
汇报人: 凌国玮

Concretely Efficient Secure Multi-party Computation Protocols: Survey and More Semi-honest Part

作者: DG Feng, K Yang

Security and Safety (S&S)

MPC起源



MPC allows n parties to jointly compute the following function:

$$(y_1, \ldots, y_n) \leftarrow f(x_1, \ldots, x_n),$$

1. **Garbled circuit**
2. **Secret sharing**

Yao A C. Protocols for secure computations[C]//23rd annual symposium on foundations of computer science (SFCS 1982). IEEE, 1982: 160-164.
Yao A C. How to generate and exchange secrets[C]//27th Annual Symposium on Foundations of Computer Science (SFCS 1986). IEEE, 1986: 162-167.
Lindell Y, Pinkas B. A proof of security of Yao's protocol for two-party computation[J]. Journal of cryptology, 2009, 22(2): 161-188.

Araki T, Furukawa J and Lindell Y et al. High-throughput semi-honest secure three-party computation with an honest majority. ACM CCS 2016, 805-17.

MPC的应用（一）

ML	SecureML: A system for scalable privacy-preserving machine learning. IEEE S&P 2017. ABY3: A mixed protocol framework for machine learning. CCS 2018 GAZELLE: A low latency framework for secure neural network inference. USENIX Security 2018. XONN: XNOR-based oblivious deep neural network inference. USENIX Security 2019. QUOTIENT: Two-party secure neural network training and prediction. CCS 2019 Make some ROOM for the zeros: data sparsity in secure distributed machine learning. CCS 2019 Trident: Efficient 4PC framework for privacy-preserving machine learning. NDSS 2020. BLAZE: Blazing fast privacy-preserving machine learning. NDSS 2020 CrypTFlow: secure TensorFlow inference. IEEE S&P 2020. Delphi: A cryptographic inference service for neural networks. USENIX ATC 2020 CrypTFlow2: practical 2-party secure inference. CCS 2020 ABY2: Improved Mixed-Protocol Secure Two-Party Computation. USENIX Security 2021 SiRNN: A math library for secure RNN inference. IEEE S&P 2021 CryptGPU: fast privacy-preserving machine learning on the GPU. IEEE S&P 2021
FL	Helen: maliciously secure competitive learning for linear models. IEEE S&P 2019 Non-interactive, secure variable aggregation for decentralized, privacy-preserving learning. ACISP 2021 SAFELearn: Secure Aggregation for private Federated Learning. IEEE S&P Workshop 2021 Cerebro: A Platform for Multi-party Cryptographic Collaborative Learning. USENIX Security 2021
Data mining	Privacy-preserving data mining. CRYPTO 2000 SEPIA: Privacy-preserving aggregation of multi-domain network events and statistics. USENIX Security 2010. High-performance, secure multi-party computation for data mining applications. International Journal of Information Security 2012
Auction	A system for secure multi-party computation. CCS 2008 MASCOT: Faster malicious arithmetic secure computation with oblivious transfer. CCS 2016
Genomic analysis	Towards practical privacy for genomic computation. . IEEE S&P 2008 Secure genome-wide association analysis using multiparty computation. Nature Biotechnol 2018 Deriving genomic diagnoses without revealing patient genomes. Science 2017
Blockchain	Founding digital currency on secure computation. CCS 2014 Private liquidity matching using MPC. CT RSA 2017 Anonymous payment channels for decentralized currencies. CCS 2017

MPC的应用(二)

non-interactive (ZK)	Zero-knowledge from secure multiparty computation. STOC 2007 ZKBoo: Faster zero-knowledge for Boolean circuits. USENIX Security. 2017 Post-quantum zero-knowledge and signatures from symmetric-key primitives. CCS 2017 Lightweight sublinear arguments without a trusted setup. CCS 2017 Improved non-interactive zero knowledge with applications to post-quantum signatures. CCS 2018 Ligero++: A new optimized sublinear IOP. CCS 2020 Limbo: Ecient zero-knowledge mpcith-based arguments. CCS 2021
scalable ZK	Zero-knowledge using garbled circuits: how to prove non-algebraic statements efficiently. CCS 2013 Privacy-free garbled circuits with applications to efficient zero-knowledge. EUROCRYPT 2015 Privacy-free garbled circuits for formulas: size zero and information-theoretic. CRYPTO 2017 Mystique: Efficient Conversions for Zero-knowledge Proofs with Applications to Machine Learning. USENIX Security. 2017 Mac'n'cheese: Zero-knowledge proofs for arithmetic circuits with nested disjunctions. CRYPTO 2020 Stacked garbling for disjunctive zero-knowledge proofs. EUROCRYPT 2020 Appenzeller to brie: Efficient zero-knowledge proofs for mixed-mode arithmetic and Z_{2^k}. CCS 2021 Wolverine: Fast, Scalable, and Communication-efficient Zero-knowledge Proofs for Boolean and Arithmetic Circuits. IEEE S&P 2021 Quicksilver: Efficient and Affordable Zero-knowledge Proofs for Circuits and Polynomials Over Any Field. CCS 2021
threshold cryptography	Fast distributed RSA key generation for semi-honest and malicious adversaries. CRYPTO 2018 Secure two-party threshold ECDSA from ECDSA assumptions. IEEE S&P 2018 Fast secure multiparty ECDSA with practical distributed key generation and applications to cryptocurrency custody. CCS 2018 Threshold ECDSA from ECDSA assumptions: The multiparty case. IEEE S&P 2019 Efficient RSA key generation and threshold paillier in the two-party setting. Journal of cryptology, 2019 UC non-interactive, proactive, threshold ECDSA with identifiable Aborts. CCS 2020 Multiparty generation of an RSA modulus. CRYPTO 2020 Lightweight, scalable RSA modulus generation with a dishonest Majority. IEEE S&P 2021
PSI	Efficient circuit-based PSI via cuckoo hashing. EUROCRYPT 2018 SpOT-light: lightweight private set intersection from sparse OT extension. CRYPTO 2019 Efficient circuit-based PSI with linear communication. EUROCRYPT 2019 PSI from Paxos: fast, malicious private set intersection. EUROCRYPT 2020 Oblivious key-value stores and applications for private set intersection. CRYPTO 2021 VOLE-PSI: fast OPRF and Circuit-PSI from Vector-OLE. EUROCRYPT 2021

Security Model

- **Semi-honest:** Semi-honest adversaries (a.k.a., passive adversaries) follow the protocol specification but may try to learn more than allowed from the protocol transcript;
- **Malicious:** Malicious adversaries (a.k.a., active adversaries) can run an arbitrary attack strategy in its attempt to break the protocol.

dishonest majority ($n/2 \leq t < n$, particularly we often adopt $t = n - 1$)

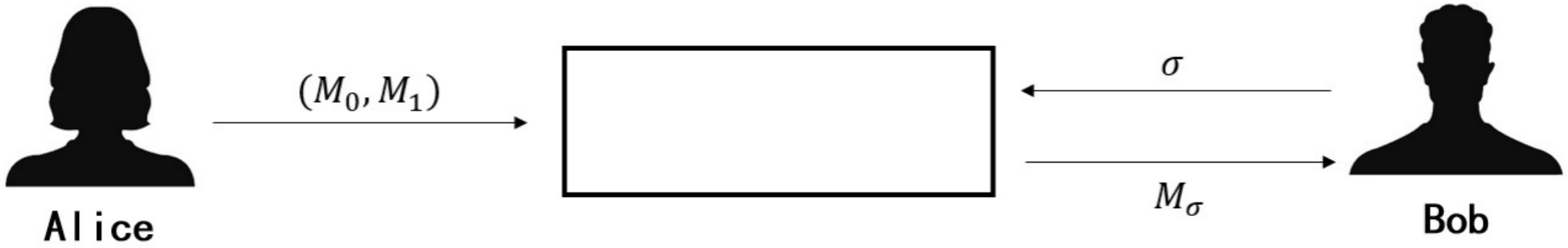
honest majority ($t < n/2$), where n is the total number of parties.

Definition 4. *Π securely realizes $\mathcal{F}_\Pi$ in the presence of semi-honest adversaries if there exists two simulators $\{\text{SIM}^\Pi_{\mathcal{P}_i}\}$ such that*

$$\text{SIM}^\Pi_{\mathcal{P}_i}(1^\kappa, x_i, \mathcal{F}_i(x_1, x_2)) \approx \text{VIEW}^\Pi_{\mathcal{P}_i}(1^\kappa, x_1, x_2), \quad (1)$$

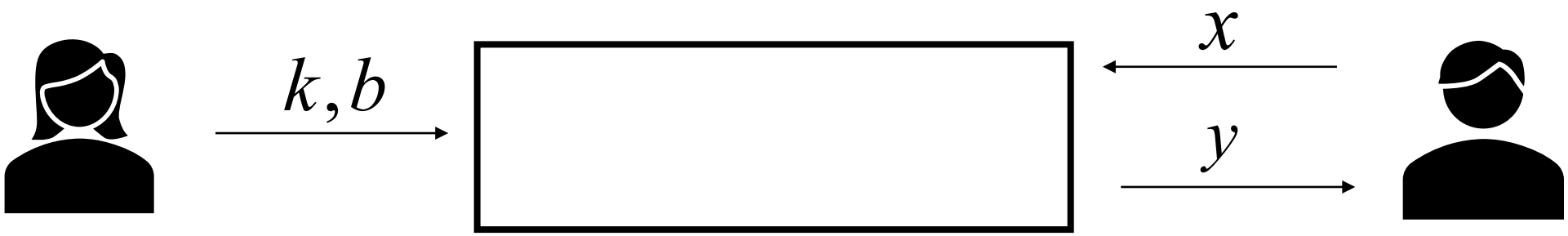
where $\approx$ denotes computational indistinguishability with respect to the security parameter κ.

Oblivious Transfer (OT)



DDH-based OT	A framework for efficient and composable oblivious transfer. CRYPTO 2008 Endemic oblivious transfer. CCS 2019 Blazing fast OT for three-round UC OT extension. CCS 2020 Minimal symmetric PAKE and 1-out-of-N OT from programmable-once public functions. CCS 2020 Batching Base Oblivious Transfers. ASIACRYPT 2021
CDH-based OT	Efficient oblivious transfer protocols. SODA 2001 Two-round oblivious transfer from CDH or LPN. EUROCRYPT 2020 Batching Base Oblivious Transfers. ASIACRYPT 2021
LWE-based OT	A framework for universally composable oblivious transfer from one-round key-exchange. IMACC 2019 Endemic oblivious transfer. CCS 2019 UC-secure OT from LWE, Revisited. SCN 2020 Batching Base Oblivious Transfers. ASIACRYPT 2021
LPN-based OT	Two-round oblivious transfer from CDH or LPN. EUROCRYPT 2020
CSIDH-based OT	Compact, Efficient and UC-secure Isogeny-based Oblivious Transfer. EUROCRYPT 2021

Oblivious Linear-function Evaluation (OLE)



OT-based OLE	MASCOT: Faster malicious arithmetic secure computation with oblivious transfer. CCS 2016 Two-party RSA key generation. CRYPTO 2019
AHE-based OLE	Overdrive: making SPDZ great again. EUROCRYPT 2018
SHE-based OLE	Multiparty computation from somewhat homomorphic encryption. CRYPTO 2012 Practical covertly secure MPC for dishonest majority or: Breaking the SPDZ limits. ESORICS 2013
RLWE-based OLE	Two-Round Oblivious Linear Evaluation from Learning with Errors. PKC 2022
RS based OLE	Oblivious transfer and polynomial evaluation. STOC 1999 Secure arithmetic computation with no honest majority. TCC 2009 Maliciously secure oblivious linear function evaluation with constant overhead. ASIACRYPT 2017
Paillier-based OLE	Reusable non-interactive secure computation. CRYPTO 2019
LPN-based OLE	Efficient pseudorandom correlation generators: Silent OT extension and more. CRYPTO 2019 Efficient pseudorandom correlation generators from ring-LPN. CRYPTO 2020

Oblivious Transfer Extension (OTE)

OTE	Correlated pseudorandomness and the complexity of private. STOC 1996
INKP-framework	Extending oblivious transfers efficiently. CRYPTO 2003 More efficient oblivious transfer and extensions for faster secure computation. CCS 2013 More efficient oblivious transfer extensions with security for malicious adversaries. EUROCRYPT 2015 Actively secure OT extension with optimal overhead. CRYPTO 2015 STOA
PCG-framework	Compressing vector OLE. CCS 2018 Efficient two-round OT extension and silent non-interactive secure computation. CCS 2019 STOA Efficient pseudorandom correlation generators: Silent OT extension and more. CRYPTO 2019 Ferret: fast extension for correlated OT with small communication. CCS 2020 STOA Correlated pseudorandom functions from variable-density LPN. FOCS 2020 （n>2^48为 STOA） Silver: silent VOLE and oblivious transfer from hardness of decoding structured LDPC codes. CRYPTO 2021 STOA 安全性有待商榷

Vector Oblivious Linear-function Evaluation （VOLE）

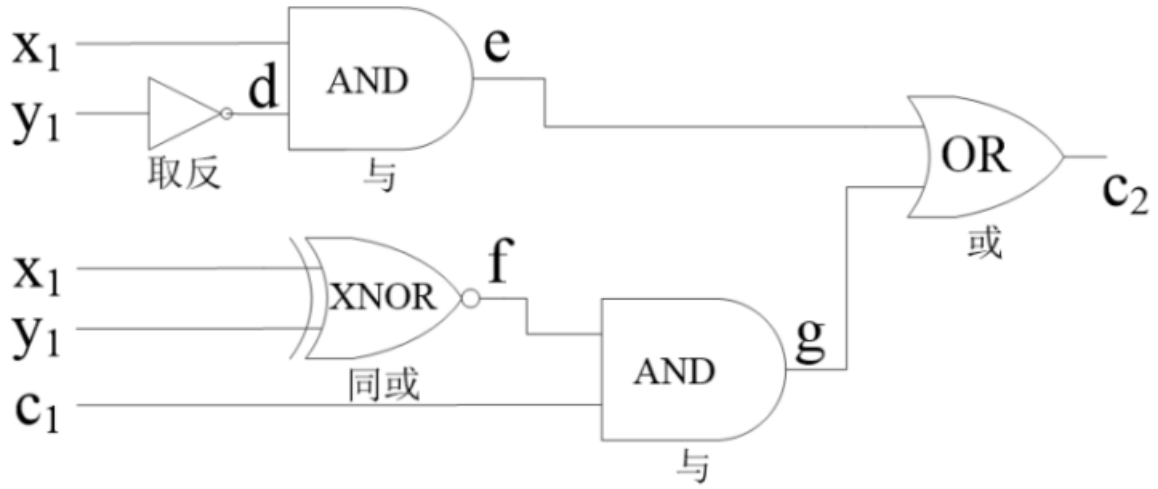
OTE to VOLE	Faster malicious arithmetic secure computation with oblivious transfer. CCS 2016
AHE-based VOLE	Overdrive: making SPDZ great again. EUROCRYPT 2018
PCG-framework	Compressing vector OLE. CCS 2018 Distributed vector-OLE: Improved constructions and implementation. CCS 2019 Efficient pseudorandom correlation generators: Silent OT extension and more. CRYPTO 2019 Efficient two-round OT extension and silent non-interactive secure computation. CCS 2019 STOA Ferret: fast extension for correlated OT with small communication. CCS 2020 STOA Correlated pseudorandom functions from variable-density LPN. FOCS 2020 （n>2^48为 STOA） Silver: silent VOLE and oblivious transfer from hardness of decoding structured LDPC codes. CRYPTO 2021 STOA 安全性有待商榷 Wolverine: Fast, Scalable, and Communication-efficient Zero-knowledge Proofs for Boolean and Arithmetic Circuits. IEEE S&P 2021

MPC的奠基（20世纪80年代）

GC	Yao A C. Protocols for secure computations[C]//23rd annual symposium on foundations of computer science (SFCS 1982)
BGW	Goldwasser S, Ben-Or M, Wigderson A. Completeness theorems for non-cryptographic fault-tolerant distributed computing (STOC 1988)
GMW	Goldreich O, Micali S and Wigderson A. How to play any mental game or A completeness theorem for protocols with honest majority (STOC 1987)
Distributed GC	Beaver D, Micali S and Rogaway P. The round complexity of secure protocols (STOC 1990)
	Ben-Or M, Goldwasser S and Wigderson A. Completeness theorems for non-cryptographic fault-tolerant distributed computation (STOC 1988)
	Chaum D, Crepeau C and Damgard I. Multiparty unconditionally secure protocols (STOC 1988)

Garbled circuit （—）

$$c_{i+1} = \begin{cases} 1, & x_i x_{i-1} \ldots x_1 > y_i y_{i-1} \ldots y_1 \\ 0, & x_i x_{i-1} \ldots x_1 \le y_i y_{i-1} \ldots y_1 \end{cases}$$



y_1	d
1	0
0	1

取反

x_1	d	e
0	0	0
0	1	0
1	0	0
1	1	1

与

x_1	y_1	f
0	0	1
0	1	0
1	0	0
1	1	1

同或

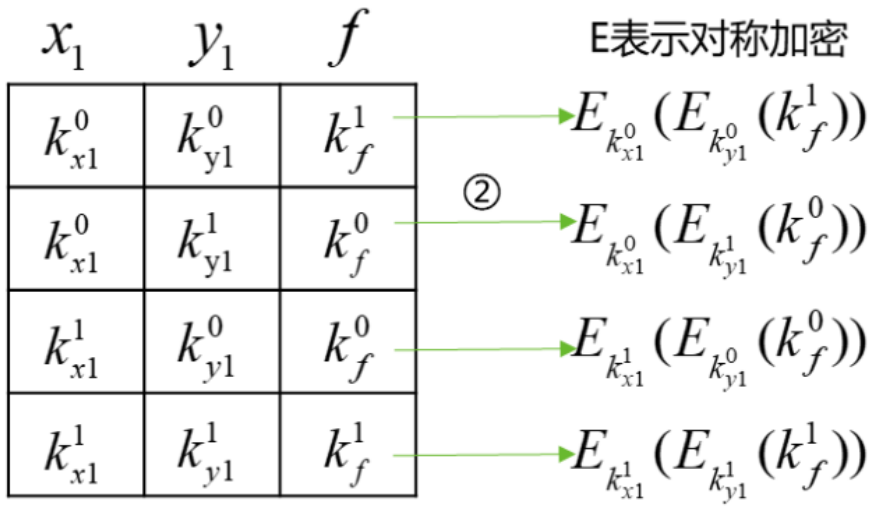
c_1	f	g
0	0	0
0	1	0
1	0	0
1	1	1

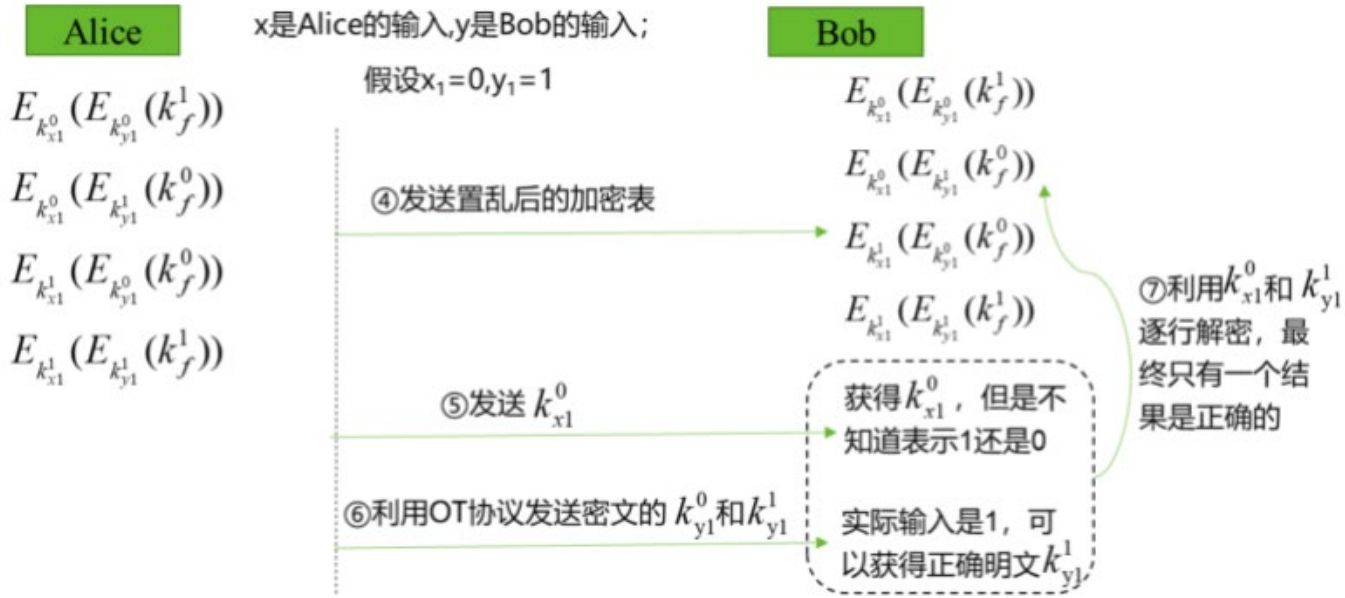
与

e	g	c_2
0	0	0
0	1	1
1	0	1
1	1	1

或

Garbled circuit （二）





Linear Secret Sharing (SS)

Additive SS	$t=n-1$	
Shamir SS	$t<n$	Shamir SS is mainly used for a large n in the honest-majority MPC protocols.
Replicated SS	$t<n$	we mainly use replicated secret sharing when n is small.
Beaver Triplets	$C1+C2 = (X1+X2)(Y1+Y2)$ $C1+C2=XY$	Secure multiplication

Shamir SS:
Shamir A. How to share a secret. Commun ACM 1979; 22: 612-3.
Replicated SS:
Cramer R, Damgard I and Ishai Y. Share conversion, pseudorandom secret-sharing, and applications to secure computation. TCC 2005, 342-62.
Ito M, Saito A and Nishizeki T. Secret sharing scheme realizing general access structure. Electron Commun 1989; 72: 56-64.
Lindell Y and Nof A. A framework for constructing fast MPC over arithmetic circuits with malicious adversaries and an honest majority. CCS 2017, 259-76.
Beaver Triplets:
Beaver D. Efficient multiparty protocols using circuit randomization. CRYPTO 1992, 420-32.
Mouchet C, Troncoso-Pastoriza J and Bossuat J-P et al. Multiparty Homomorphic Encryption from Ring-learning-with-errors. PETS 2021.

Semi-honest protocols based on SS

GMW	ASS	GMW vs. Yao? Efficient secure two-party computation with low-depth circuits. FC 2013 Circuits resilient to additive attacks with applications to secure computation. STOC 2014 (bool to arithmetic) More efficient oblivious transfer and extensions for faster secure computation. CCS 2013 Pushing the communication barrier in secure computation using lookup tables. NDSS 2017 STOA TinyKeys: A new approach to efficient multi-party computation. CCS 2018 STOA
BGW	Shamir SS	Simplified VSS and fast-track multiparty computations with applications to threshold cryptography. PODC 1998 Scalable and unconditionally secure multiparty computation. CRYPTO 2007 Efficient information-theoretic secure multiparty computation over Z=pkZ via galois rings. TCC 2019 (Z_p to Z_{2^k}) ATLAS: Efficient and scalable MPC in the honest majority setting. CRYPTO 2021 STOA
3PC	Replicated SS	GMW High-throughput semi-honest secure three-party computation with an honest majority. CCS 2016 A framework for constructing fast MPC over arithmetic circuits with malicious adversaries and an honest-majority. CCS 2017 (bool to arithmetic)
4,5 PC	Replicated SS	Zero-knowledge proofs on secret-shared data via fully linear PCPs. CRYPTO 2019 Efficient fully secure computation via distributed zero-knowledge proofs. ASIACRYPT 2020 STOA Fantastic four: Honest-majority four-party secure computation with malicious security. USENIX Security 2021

Semi-honest two-party computation based on GC

1982	Yao	Protocols for secure computations (**提出了百万富翁问题，并给出了非常简单的解决办法**)	SFCS
1986	Yao	How to generate and exchange secrets (**将百万富翁问题扩展到了任意的f**)	SFCS
1990	Beaver	The round complexity of secure protocols (**降低了Yao 86的通信量, 从8k到4k**)	STOC
1995	Beaver	Precomputing oblivious transfer (**通过预计算OT提高效率)**	CRYPTO
1999	Naor, Pinkas, et al.	Privacy-preserving auctions and mechanism design (**4k to 3k**)	EC
2008	Kolesnikov et al.	Improved garbled circuit: Free XOR gates and applications. (**直接让加法门没有了通信开销**)	ICALP
2009	Pinkas et al.	Secure two-party computation is practical. (**3k to 2k，但加法门有通信**)	ASIACRYPT
2009	Lindell and Pinkas	A proof of security of Yao's protocol for two-party computation **(Yao 86的正式定义以及安全性证明)**	Journal of cryptology
2011	Huang et al.	Faster secure two-party computation using garbled circuits (**实现了电路的批处理**)	USENIX Security
2012	Choi et al.	On the security of the "free-XOR" technique (**去掉加法门通信技术的安全性分析**)	TCC
2012	Bellare et al.	Foundations of garbled circuits (**混淆电路的正式定义**)	CCS
2014	Kolesnikov et al.	FleXOR: Flexible garbling for XOR gates that beats free-XOR	CRYPTO
2015	Gueron, Lindell et al.	Fast garbling of circuits under standard assumptions	CCS
2015	Zahur, Rosulek et al.	Two halves make a whole reducing data transfer in garbled circuits using half gates. **(2k 且加法门无通信)**	EUROCRYPT
2021	Rosulek and Roy.	Three halves make a whole? Beating the half-gates lower bound for garbled circuits. (**1.5k+5** STOA)	CRYPTO

Applebaum B, Ishai Y and Kushilevitz E. How to garble arithmetic circuits. FOCS 2011
Ball M, Malkin T and Rosulek M. Garbling gadgets for Boolean and arithmetic circuits. CCS 2016
Ben-Efraim A. On multiparty garbling of arithmetic circuits. ASIACRYPT 2018

Semi-honest multi-party computation based on GC

1990	Beaver, Micali and Rogaway	The round complexity of secure protocols (**第一个多方计算协议，BMR style**)	STOC
2016	Ben-Efraim, Lindell, and Omri	Optimizing semi-honest secure multiparty computation for the Internet	CCS
2017	Wang, Ranellucci, and Katz	Global-scale secure multiparty computation (**WRK style**)	CCS
2017	Aner Ben-Efraim, Lindell and Omri	Efficient scalable constant-round MPC via garbled circuits (n>100,但不能xor-free)	ASIACRYPT
2020	Yang, Wang, and Zhang	More efficient MPC from improved triple generation and authenticated garbling (STOA)	CCS
2021	Ben-Efraim, Cong, and Omri et al.	Large scale, actively secure computation from LPN and free-XOR garbled circuits n>100	EUROCRYPT

MPC application to machine learning (dishonest-majority)

SecureML: A system for scalable privacy-preserving machine learning	两方	IEEE S&P 2017
Helen: maliciously secure competitive learning for linear models	多方	IEEE S&P 2019
Secure evaluation of quantized neural networks	两方	PETS 2020
CrypTFlow2: practical 2-party secure inference	两方 STOA	CCS 2020
Cerebro: A Platform for Multi-party Cryptographic Collaborative Learning. **(任意的ML任务,和最新的NN，但效率较低)**	多方	USENIX Security 2021

MPC application to machine learning (honest-majority)

SecureML: A system for scalable privacy-preserving machine learning	三方	IEEE S&P 2017
CryptGPU: fast privacy-preserving machine learning on the GPU	三方	IEEE S&P 2021
FALCON: Honest-majority Maliciously Secure Framework for Private Deep Learning（**恶意, 非常慢**）	四方	2020 未发表
Tetrad: Actively Secure 4 PC for Secure Training and Inference	四方	2021 未发表
Cerebro: A Platform for Multi-party Cryptographic Collaborative Learning. **(任意的ML任务,和最新的NN，但效率较低)**	多方	USENIX Security 2021

Table 3. Comparison of various PPML protocols

	PPML	Capability		Threat Model		Techniques	Neural Networks
		Inference	Training	Semi-honest	Malicious		
2PC	SecureML [24]	√	√	√		HE/GC/ASS	From [24]
2PC	MiniONN [277]	√		√		HE/GC/ASS	From [24, 277]
2PC	GAZELLE [20]	√		√		HE/GC/ASS	From [24, 277]
2PC	EzPC [278]	√		√		GC/ASS	From [24, 277]
2PC	XONN [29]	√		√		GC/ASS	VGG-16 [279]
2PC	QUOTIENT [18]	√	√	√		OT/GC/ASS	From [18]
2PC	MP2ML [280]	√		√		HE/GC/ASS	CryptoNets [281]
2PC	CrypTFlow2 [28]	√		√		HE/OT/ASS	DenseNet-121 [282]
2PC	Delphi [22]	√		√		HE/GC/ASS	VGG-16 [279]
2PC	QuantizedNN [283]	√		√	Abort	HE/OT/ASS	MobileNets [284]
2PC	SIRNN [27]	√		√		OT/ASS	Heads [285]
3PC	Chameleon [286]	√		√		GC/ASS	AlexNet [287]
3PC	ABY^3 [23]	√	√	√		GC/ASS	From [24, 277]
3PC	ASTRA [288]	√	√	√	Abort	ASS/RSS	From [24]
3PC	SecureNN [289]	√	√	√		ASS	From [24, 277]
3PC	BLAZE [26]	√	√	√	Fairness	ASS/RSS	From [24]
3PC	QuantizedNN [283]	√		√	Abort	RSS	MobileNets [284]
3PC	CrypTFlow [21]	√		√		ASS	DenseNet-121 [282]
3PC	SWIFT [290]	√	√	√	GOD	ASS/RSS	VGG-16 [279]
3PC	CryptGPU [31]	√	√	√		RSS	ResNet-152 [291]
3PC	Falcon [292]	√	√	√	Abort	RSS	VGG-16 [279]
4PC	FLASH [293]	√	√	√	GOD	ASS/RSS	From [24]
4PC	SWIFT [290]	√	√	√	GOD	ASS/RSS	VGG-16 [279]
4PC	Trident [19]	√	√	√	Fairness	GC/ASS/RSS	From [24]
4PC	Tetrad [294]	√	√	√	GOD	GC/ASS/RSS	VGG-16 [279]

MPC Libraries

ABY	ABY. A framework for efficient mixed-protocol secure two-party computation. NDSS 2015
EMP-toolkit	https://github.com/emp-toolkit
FRESCO	https://github.com/aicis/fresco
JIFF	https://github.com/multiparty/ji
MP-SPDZ	A versatile framework for multi-party computation. CCS 2020
MPyC	https://github.com/lschoe/mpyc.
SCALEMAMBA	https://github.com/KULeuven-COSIC/SCALE-MAMBA.
Bogdanov et al.	Sharemind: A framework for fast privacy-preserving computations. ESORICS 2008
TinyGable	TinyGarble: highly compressed and scalable sequential garbled circuits. IEEE S&P 2015

各个库的比较： Hastings M, Hemenway B and Noble D et al. SoK: General purpose compilers for secure multi-party computation. IEEE S&P 2019
Keller M. MP-SPDZ: A versatile framework for multi-party computation. CCS 2020