# 秘密分享

**如何设计搜索关键字：**

* + 1. Secret sharings
    2. Secure multi-party computation
    3. GMW protocol
    4. BGW protocol
    5. SPDZ
    6. BDOZ
    7. Verifiable secret sharing
    8. Publicly verifiable secret sharing

**使用哪种搜索手段通过什么知识源收集来多少相关的文章：**

* + 1. DBLP：<https://dblp.org>
    2. google scholar：https://scholar.google.com.hk/?hl=zh-CN
    3. semantic scholar：<https://www.semanticscholar.org/me/research>
    4. connected papers：https://www.connectedpapers.com

**这些文章按照哪些维度分成多少子类别：**

1.秘密分享SS

1.1semi-honest协议

* + 1. GMW协议

Goldreich等人（1987）提出的GMW方案是基于加法秘密分享的MPC方案，它可以处理n≥2的所有情况，原生的GMW只考虑了布尔电路但也可扩展到算术电路上。在计算加法门时，各参与方将自己的共享份额相加即可，不需要交互。而在计算乘法门时，原生的GMW方法交互次数及计算量都很高，无法用于实际计算。

Goldreich O, Micali S and Wigderson A. How to play any mental game or A completeness theorem for protocols with honest majority. In: Aho A (ed.). 19th ACM STOC. ACM Press, 1987, 218–29

Beaver等人(1992)提出一种方法，利用一种随机选取的Beaver三元组，可以将乘法门计算分为预计算与在线计算两个阶段，大量的交互操作都转移到预计算过程中，在线计算过程中只需要1次交互即可。

BEAVER D. Efficient multiparty protocols using circuit randomization[C]. Annual International Cryptology Conference, Santa Barbara, USA, 1992: 420–432.

Schneider等人（2013）提出由于GMW协议需要交互来对AND门进行安全计算，因此可以通过使用具有小的尺寸和深度的电路来减少延迟。同时通过负载均衡和并行处理多个门来优化GMW协议，提供了双方的情况下的性能。

Schneider T and Zohner M. GMW vs. Yao? Efficient secure two-party computation with low depth circuits. In: Sadeghi A-R (ed.). FC 2013, volume 7859 of LNCS. Heidelberg: Springer, 2013, 275–92.

Dessouky等人（2017）首先将具有两个输入门的布尔电路的通信性能提高了1.9倍。同时进一步将传统的布尔电路表示从两输入门改变为多输入/多输出查找表(LUT)，可以编程实现任意功能。构造了两个用于计算LUT的协议，提供了在线通信和整体通信之间的权衡。

Dessouky G, Koushanfar F and Sadeghi A-R et al. Pushing the communication barrier in secure computation using lookup tables. In: NDSS 2017. The Internet Society, 2017

Hazay等人（2018）提出如果允许n/2≤t<n-1(仍是不诚实大多数)，可以使用TinyKeys方法来改进多二进制域上的协议的效率。使用带有短密钥的IKNP OT扩展协议来生成Beaver乘法三元组。其基本思想是，尽管诚实各方的短密钥只具有较低的熵，但诚实各方的短密钥的组合将具有较大的熵。

Hazay C, Orsini E and Scholl P et al. TinyKeys: A new approach to efficient multi-party computation. In: Shacham H and Boldyreva A (eds.). CRYPTO 2018, Part III, volume 10993 of LNCS. Heidelberg: Springer, 2018, 3–33.

* + 1. BGW协议

Ben等人（1988）提出的BGW协议是一个基于Shamir秘密共享的多方安全计算方案。它将计算函数解析成算术电路，然后逐门计算，支持模p下的数乘、加法和乘法运算。

Ben-Or M, Goldwasser S and Wigderson A. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In: 20th ACM STOC. ACM Press, 1988, 1–10.

当参与方的数量很少(特别是n<=5)时，主要采用Gennaro等人（1998）提出的使用降阶方法的GRR协议来实现乘法。GRR协议的工作方式是让每一方在本地将输入[x]，[y]的份额相乘，将结果共享给所有其他方(允许将多项式的次数从2t降低到t)，然后在本地计算份额的线性组合作为其在输出[z]中的份额。

Gennaro R, Rabin MO and Rabin T. Simplified VSS and fast-track multiparty computations with applications to threshold cryptography. In: Coan BA and Afek Y (eds.). 17th ACM PODC. ACM, 1998, 101–111.

当参与方的数量较大(例如n>5)，主要采用Damg˚ard等人（2007）提出的DN协议来实现两个秘密值的相乘。原始DN协议每一方每个乘法门需要六个通信元素。Goyal等人（2020）首先改进了DN协议的通信开销，从6个元素降到5.5个元素。随后Goyal等人（2021）将DN协议的通信进一步改进为每方每个乘法门4个元素。此外，ATLAS提出了一种改进的DN乘法和Beaver三元乘法相结合的方法，将轮数复杂度降低了2倍，而每一方的每个乘法门的通信开销额外增加了0.5个元素。

Damg˚ard I and Nielsen JB. Scalable and unconditionally secure multiparty computation. In: Menezes A (ed.). CRYPTO 2007, volume 4622 of LNCS. Heidelberg: Springer, 2007, 572–90.

Goyal V and Song Y. Malicious security comes free in honest-majority MPC. Cryptology ePrint Archive, Report 2020/134, 2020. <https://eprint.iacr.org/2020/134.>

Goyal V, Song Y and Zhu C. Guaranteed output delivery comes free in honest majority MPC. In: Micciancio D and Ristenpart T (eds.). CRYPTO 2020, Part II, volume 12171 of LNCS. Heidelberg: Springer, 2020, 618–46.

Goyal V, Li H and Ostrovsky R et al. ATLAS: Efficient and scalable MPC in the honest majority setting. In: Advances in Cryptology – CRYPTO 2021. Springer, 2021.

Abspoel等人（2021）提出了一个新的观点，使用再生码构造了单轮乘法协议，代价是将通信复杂度增加了O(n/logn)倍，其中Shamir秘密共享的再生性要求参与方n的数量很大，并且DN乘法协议需要大约两轮。

Abspoel M, Cramer R and Escudero D et al. Improved single-round secure multiplication using regenerating codes. Cryptology ePrint Archive, Report 2021/253, 2021. <https://eprint.iacr.org/2021/253.>

* 1. maliciously secure协议
     1. 不诚实大多数

GMW提出了一个通用编译器，用于将半诚实的MPC协议转换为恶意安全的MPC协议。然而，该编译器是非黑盒的，在每一步都使用通用的零知识证明来证明计算的正确性，因此并不是很有效。

IPS(2008)提出了一个黑盒编译器，其中内部具有半诚实安全性的MPC协议在OT-混合模型中计算电路，而外部MPC协议在诚实多数情况下具有恶意安全性，以保证整个MPC协议在恶意攻击者存在的情况下的安全性。

Ishai Y, Prabhakaran M and Sahai A. Founding cryptography on oblivious transfer – efficiently. In: Wagner D (ed.). CRYPTO 2008, volume 5157 of LNCS. Heidelberg: Springer, 2008, 572–91.

Lindell等人（2011）提出了对IPS编译器在多方情况下的改进，Ames等人（2017）和Hazay等人（2019）中针对两方的情况进行了进一步优化。然而，基于IPS编译器的恶意安全MPC协议的具体效率(concrete efficiency)还不够高。

Lindell Y, Oxman E and Pinkas B. The IPS compiler: optimizations, variants and concrete efficiency. In: Rogaway P (ed.). CRYPTO 2011, volume 6841 of LNCS. Heidelberg: Springer, 2011, 259–76.

Ames S, Hazay C and Ishai Y et al. Ligero: Lightweight sublinear arguments without a trusted setup. In: Thuraisingham BM, Evans D, Malkin T, Xu D (eds.). ACM CCS 2017. ACM Press, 2017, 2087–2104.

Hazay C, Ishai Y and Marcedone A et al. LevioSA: Lightweight secure arithmetic computation. In: Cavallaro L, Kinder J, Wang XF and Katz J (eds.). ACM CCS 2019. ACM Press, 2019, 327–44.

Hazay等人（2020）基于IPS框架提出了一种新的两层共享编译器，外层为Shamir秘密共享或代数几何(AG)秘密共享，内层为加法秘密共享。他们的编译器允许任意大小的域，在半诚实的GMW协议上具有恒定的通信开销，但具体效率仍然很低。

Hazay C, Venkitasubramaniam M and Weiss M. The price of active security in cryptographic protocols. In: Canteaut A and Ishai Y (eds.). EUROCRYPT 2020, Part II, volume 12106 of LNCS. Heidelberg: Springer, 2020, 184–215.

Boyle等人（2021）新颖地使用了Boneh等人（2019）的技术，以前仅在诚实大多数MPC中使用。通过预处理保护MPC免受恶意方的攻击，可以被视为GMW编译器的亚线性信息论变体，它适用于具有预处理的MPC的自然协议。

Boyle, E., Gilboa, N., Ishai, Y., Nof, A. (2021). Sublinear GMW-Style Compiler for MPC with Preprocessing. In: Malkin, T., Peikert, C. (eds) Advances in Cryptology – CRYPTO 2021. CRYPTO 2021. Lecture Notes in Computer Science(), vol 12826. Springer, Cham. https://doi.org/10.1007/978-3-030-84245-1\_16

在不诚实大多数的情况下中，为了实现恶意安全，需要引入IT-MAC。目前，在MPC协议中使用的IT-MAC有两种：BDOZ-Style 和SPDZ-Style。大多数MPC研究都集中在提高预处理阶段的效率上，而生成认证三元组是效率瓶颈。对于认证三元组的生成，考虑两种情况：

1. 大域

Damg˚ard等人（2012、2013）提出的SPDZ框架是不诚实大多数且恶意情况下最先进的协议。原始SPDZ协议在预处理阶段使用深度1同态加密(HE)方案(即底层HE方案可以支持一次乘法)来生成认证的三元组，并且可以在在线阶段快速地评估电路。

Damg˚ard I, Pastro V, Smart NP and Zakarias S. Multiparty computation from somewhat homomorphic encryption. In: Safavi-Naini R and Canetti R (eds.). CRYPTO 2012, volume 7417 of LNCS. Heidelberg: Springer, 2012, 643–62.

Damg˚ard I, Keller M and Larraia E et al. Practical covertly secure MPC for dishonest majority – or: Breaking the SPDZ limits. In: Crampton J, Jajodia S and Mayes K (eds.). ESORICS 2013, volume 8134 of LNCS. Heidelberg: Springer, 2013, 1–18.

Keller等人（2016）提出了一种称为MASCOT的SPDZ-style的协议，该协议使用OT扩展协议和Gilboa乘法思想来更有效地生成认证三元组。

Keller M, Orsini E and Scholl P. MASCOT: Faster malicious arithmetic secure computation with oblivious transfer. In: Weippl ER, Katzenbeisser S, Kruegel C, Myers AC and Halevi S (eds.). ACM CCS 2016. ACM Press, 2016, 830–42.

Keller等人（2018）基于加性同态加密和基于格的零知识证明提出了一种优化的SPDZ-style的协议OverDrive，该协议显著改善了通信以生成可认证的三元组。OverDrive包括两个版本：Low Gear适用于少数参与方，High Gear适用于很多参与方。

Keller M, Pastro V and Rotaru D. Overdrive: making SPDZ great again. In: Nielsen JB and Rijmen V (eds.). EUROCRYPT 2018, Part III, volume 10822 of LNCS. Heidelberg: Springer, 2018, 158–89.

Baum等人（2019）通过优化基础零知识协议进一步改进了HighGear的性能。

Baum C, Cozzo D and Smart NP. Using TopGear in overdrive: A more efficient ZKPoK for SPDZ. In: Paterson KG and Stebila D (eds.). SAC 2019, volume 11959 of LNCS. Heidelberg: Springer, 2019, 274–302.

Chen等人（2020）将深度-2HE方案集成到SPDZ框架中，提高了SPDZ协议计算矩阵乘法和二维卷积的效率。对于其他一般功能，由于HE的参数较大，尚不清楚他们的方法是否可以实现更好的效率。

Chen H, Kim M and Razenshteyn I et al. Maliciously secure matrix multiplication with applications to private deep learning. Cryptology ePrint Archive, Report 2020/451, 2020. https://eprint.iacr.org/2020/451.

（虽然域上半诚实的GMW协议可以直接扩展到环Z2^k，但对于具有恶意安全性的SPDZ-style的协议来说，并不容易。）

Cramer等人（2018）提出了第一个具体高效的环上MPC协议SPDZ框架(称为SPDZ2^k)，在两个不同的环上使用IT-MAC，其中秘密值在Z2^k上，而MAC标记在Z2^k+s。他们的协议SPDZ2^k使用MASCOT的想法来生成经过验证的三元组，但需要比MASCOT更多的通信。

Cramer R, Damg˚ard I and Escudero D et al. SPD Z2k : Efficient MPC mod 2k for dishonest majority. In: Shacham H and Boldyreva A (eds.). CRYPTO 2018, Part II, volume 10992 of LNCS. Heidelberg: Springer, 2018, 769–98.

Damgard等人（2019）实现了SPDZ\_2^k，在环Z\_2^k上设计了新的等价性测试、比较和截断协议，并证明了使用SPDZ\_2^k在ML域上的这些操作比基于域的SPDZ-style的协议更有效。

Damg˚ard I, Escudero D and Frederiksen TK et al. New primitives for actively-secure MPC over rings with applications to private machine learning. In: 2019 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, 2019, 1102–20

随后，Catalano等人（2020）和Orsini（2020）等人基于SPDZ\_2^k思想的两个改进的MPC协议也被提出。

Catalano D, Di Raimondo M and Fiore D et al. MonZ2k a: Fast maliciously secure two party computation on Z2k . In: Kiayias A, Kohlweiss M, Wallden P and Zikas V (eds.). PKC 2020, Part II, volume 12111 of LNCS. Heidelberg: Springer, 2020, 357–86.

Orsini E, Smart NP and Vercauteren F. Overdrive2k: efficient secure MPC over Z2k from somewhat homomorphic encryption. In: Jarecki S (ed.). CT-RSA 2020, volume 12006 of LNCS. Heidelberg: Springer, 2020, 254–83.

Boyle等人（2020）基于一种新的环-LPN的变量假设，提出了几种新的在PCG框架下生成Beaver乘法三元组和认证三元组的协议。它们利用分布式点函数(DPF)和环-LPN中噪声的稀疏特性，在半诚实的两方情况中以较小的通信量产生Beaver三元组。利用PCG的可编程性，用于在两方情况下产生Beaver三元组的半诚实协议可以容易地扩展到多方设置。在构造SPDZ-style认证分享的基础上，Boyle等人还扩展了半诚实协议，以在双方恶意情况下生成认证的三元组。恶意安全协议的通信比OverDrive小两个数量级。虽然通信效率很有吸引力，但为了使PCG方法更实用，进一步降低计算成本是值得的。还给出了使用三方DPF在多方情况下生成经过验证的三元组的候选构造。但是它的具体效率很低。

Boyle E, Couteau G and Gilboa N et al. Efficient pseudorandom correlation generators from ring-LPN. In: Micciancio D and Ristenpart T (eds.). CRYPTO 2020, Part II, volume 12171 of LNCS. Heidelberg: Springer, 2020, 387–416.

2）二进制域

TinyOT-style协议中用于生成认证三元组的子协议可用于设计具有恶意安全性的常数轮MPC协议[HSS,KRR,WRK,YWZ]。这些TinyOT-style的协议采用BDOZ-style的IT-MAC来认证，并使用分组法来消除由于选择失败攻击而可能导致的份额泄漏，其中攻击者可以以1/2的概率猜测诚实方的比特份额，但将以相同的概率被捕获。

Hazay C, Scholl P and Soria-Vazquez E. Low cost constant round MPC combining BMR and oblivious transfer. In: Takagi T and Peyrin T (eds.). ASIACRYPT 2017, Part I, volume 10624 of LNCS. Heidelberg: Springer, 2017, 598–628.

Katz J, Ranellucci S and Rosulek M et al. Optimizing authenticated garbling for faster secure two-party computation. In: Shacham H and Boldyreva A (eds.). CRYPTO 2018, Part III, volume 10993 of LNCS. Heidelberg: Springer, 2018, 365–91.

Wang X, Ranellucci S and Katz J. Authenticated garbling and efficient maliciously secure two-party computation. In: Thuraisingham BM, Evans D, Malkin T and Xu D (eds.). ACM CCS 2017. ACM Press, 2017, 21–37.

Wang X, Ranellucci S and Katz J. Global-scale secure multiparty computation. In: Thuraisingham BM, Evans D, Malkin T and Xu D (eds.). ACM CCS 2017. ACM Press, 2017, 39–56.

Yang K, Wang X and Zhang J. More efficient MPC from improved triple generation and authenticated garbling. In: Ligatti J, Ou X, Katz J and Vigna G (eds.). ACM CCS 20. ACM Press, 2020, 1627–46.

Damg˚ard等人（2013）提出的MiniMAC旨在解决SPDZ对于二进制域具有很大的通信开销的问题。MiniMAC采用了批量认证的思想：如果需要一次计算同一布尔电路的k个实例，可以将这些计算捆绑在一起，并将它们视为在大环F^k上的单个布尔电路的计算，其中在F^k上的加法和乘法是按分量进行的。在MiniMAC中，消息上的IT-MAC被定义为C(x)\*\Delta，其中\Delta \in F^k。C是具有大的最小距离的线性纠错码，而\*是分量乘积。

Damg˚ard I and Zakarias S. Constant-overhead secure computation of Boolean circuits using preprocessing. In: Sahai A (ed.). TCC 2013, volume 7785 of LNCS. Heidelberg: Springer, 2013, 621–41

MiniMAC风格的MPC协议[FKO,CG,DLT,DZ,FPY]也适用于分层布尔电路，其中布尔电路的门被划分成有序层，并且层仅由相同类型的门组成。

Frederiksen TK, Keller M and Orsini E et al. A unified approach to MPC with preprocessing using OT. In: Iwata T and Cheon JH (eds.). ASIACRYPT 2015, Part I, volume 9452 of LNCS. Heidelberg: Springer, 2015, 711–35.

Cascudo I, Gundersen J-S. A secret-sharing based MPC protocol for Boolean circuits with good amortized complexity. In: Theory of Cryptography, volume 12551 of LNCS. Springer International Publishing, 2020, 652–82.

Damg˚ard I, Lauritsen R and Toft T. An empirical study and some improvements of the MiniMac protocol for secure computation. In: Abdalla M and De Prisco R (eds.). SCN 14, volume 8642 of LNCS. Heidelberg: Springer, 2014, 398–415.

Damg˚ard I and Zakarias S. Constant-overhead secure computation of Boolean circuits using preprocessing. In: Sahai A (ed.). TCC 2013, volume 7785 of LNCS. Heidelberg: Springer, 2013, 621–41.

Frederiksen TK, Pinkas B and Yanai A. Committed MPC – maliciously secure multiparty computation from homomorphic commitments. In: Abdalla M and Dahab R (eds.). PKC 2018, Part I, volume 10769 of LNCS. Heidelberg: Springer, 2018, 587–619.

其中CG的MiniMAC-style协议采用了最初为诚实多数MPC提出的称为反向乘法友好嵌入(RMFE)的代数工具，并且获得了较低的通信成本。

此外，对于较小的域，提出了TinyTable-style协议[DNNR,C19,KOR]，非常适合于使用一次性真值表方法的安全AES或3DES评估。

Damg˚ard I, Nielsen JB, Nielsen M and Ranellucci S. The TinyTable protocol for 2-party secure computation, or: Gatescrambling revisited. In: Katz J and Shacham H (eds.). CRYPTO 2017, Part I, volume 10401 of LNCS. Heidelberg: Springer, 2017, 167–87.

Couteau G. A note on the communication complexity of multiparty computation in the correlated randomness model. In: Ishai Y and Rijmen V (eds.). EUROCRYPT 2019, Part II, volume 11477 of LNCS. Heidelberg: Springer, 2019, 473–503.

Keller M, Orsini E and Rotaru D et al. Faster secure multi-party computation of AES and DES using lookup tables. In: Gollmann D, Miyaji A and Kikuchi H (eds.). ACNS 17, volume 10355 of LNCS. Heidelberg: Springer, 2017, 229–49.

1.2.2 诚实大多数

* 允许腐坏阈值t<n/2

Lindell等人（2017）观察到半诚实的DN协议在恶意攻击者存在的情况下保证了秘密值的私密性，并允许攻击者在输出中引入加法错误，例如对两个份额[x],[y]，DN协议会输出一个份额[z]，z=x\*y+d，其中d是附加错误。该观察结果也适用于GRR协议和基于复制秘密共享的乘法协议。他们采用Beaver三元组和随机线性组合的方法来检查乘法门的正确性，这与半诚实协议相比引入了相对较大的开销。

Lindell Y and Nof A. A framework for constructing fast MPC over arithmetic circuits with malicious adversaries and an honest-majority. In: Thuraisingham BM, Evans D, Malkin T and Xu D (eds.). ACM CCS 2017. ACM Press, 2017, 259–76.

Chida等人（2018）提出了一种不同的方法来验证乘法门的正确性，其中半诚实乘法协议被执行两次，然后各方使用另一个相关的乘法三元组来检查乘法门的正确性。与半诚实的DN协议相比，他们的MPC协议仍然引入了两倍的通信开销。

Chida K, Genkin D and Hamada K et al. Fast large-scale honest-majority MPC for malicious adversaries. In: Shacham H and Boldyreva A (eds.). CRYPTO 2018, Part III, volume 10993 of LNCS. Heidelberg: Springer, 2018, 34–64.

同时，Nordholt和Veeningen（2018）也实现了两倍的通信开销。

Nordholt PS and Veeningen M. Minimising communication in honest-majority MPC by batchwise multiplication verification. In: Preneel B and Vercauteren F (eds.). ACNS 18, volume 10892 of LNCS. Heidelberg: Springer, 2018, 321–39.

在三方的情况下，Furukawa等人（2017）和Araki等人（2017）将用于布尔电路的半诚实协议转换为恶意安全协议，该方法将引入O(p/logN)的开销，其中N是乘法门的数目。该开销比自然重复方法小，但不是最优的。

Furukawa J, Lindell Y and Nof A et al. High-throughput secure three-party computation for malicious adversaries and an honest majority. In: Coron JS and Nielsen JB (eds.). EUROCRYPT 2017, Part II, volume 10211 of LNCS. Heidelberg: Springer, 2017, 225–55.

Araki T, Barak A and Furukawa J et al. Optimized honest-majority MPC for malicious adversaries – Breaking the 1 billion-gate per second barrier. In: 2017 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, 2017, 843–62.

* 允许腐坏阈值t<n/3

允许腐坏阈值t<n/3时具有恶意安全的MPC协议可以实现开销是1并且是最优的。具体地说，可以使用具有亚线性通信的分布式零知识证明来验证乘法门的正确性。

Boneh等人（2019）使用这种零知识证明和具有复制秘密共享的DN协议的变体，为固定数量的参与方构造了恶意安全的MPC协议。就关于布尔电路的3PC协议的摊销通信成本而言，他们的方法第一次实现了每一方每个与门1比特。他们的验证协议需要每个通信方O(n\sqrt N+n)个域元素，并使用Fiat-Shamir启发式进行常数轮次，其中n是参与方的数量。

Boneh D, Boyle E and Corrigan-Gibbs H et al. Zero-knowledge proofs on secret-shared data via fully linear PCPs. In: Boldyreva A and Micciancio D (eds.). CRYPTO 2019, Part III, volume 11694 of LNCS. Heidelberg: Springer, 2019, 67–97.

在三方情况下，Boyle等人(2019)对Boneh等人提出的3PC协议进行改进，使得具体效率显著提高。

Boyle E, Gilboa N and Ishai Y et al. Practical fully secure three-party computation via sublinear distributed zeroknowledge proofs. In: Cavallaro L, Kinder J, Wang XF and Katz J (eds.). ACM CCS 2019. ACM Press, 2019, 869–86.

Boyle等人（2020）以一种新的方式使用了分布式零知识证明，构造了一个MPC协议，该协议的开销比最好的半诚实协议具有更优的开销。他们的方法使用了一种新的见解，其中对于值x的任何秘密共享，我们可以同时将x的份额视为每个秘密份额xi本身的共享。他们的用于检查乘法三元组的验证协议需要每一方O(nlogN+n)个域元素的通信和常数轮数。

Boyle E, Gilboa N and Ishai Y et al. Efficient fully secure computation via distributed zero-knowledge proofs. In: Advances in Cryptology – ASIACRYPT 2020, volume 12493 of LNCS. Springer International Publishing, 2020, 244–76

在分布式零知识证明技术的基础上，Goyal等人（2020）提出了另一种针对乘法门的验证技术，实现了开销为1的恶意安全，验证协议每方需要O(LogN)轮和(nlogN+n)个域元素的通信。他们利用半诚实DN协议可以在相同通信代价下计算两个向量的内积，并采用递归的思想来执行乘法门的验证。Goyal等人的验证技术最初被描述为Shamir秘密共享，并且也可以用于复制秘密共享。

Goyal V, Song Y and Zhu C. Guaranteed output delivery comes free in honest majority MPC. In: Micciancio D and Ristenpart T (eds.). CRYPTO 2020, Part II, volume 12171 of LNCS. Heidelberg: Springer, 2020, 618–46.

2.可验证秘密分享（VSS）

可验证计算使得计算机能够将某些必要功能的计算外包给其他不受信任的第三方，同时保持结果的可验证性，从而迫使计算的执行者遵守协议，正确的执行协议指令。

Chor等人（1985）在秘密分享中引入了可验证性，由此产生了可验证秘密分享（VSS）。

CHOR B, GOLDWASSER S, MICALI S, et al. Verifiable secret sharing and achieving simultaneity in the presence of faults[C]//Annual Symposium on Foundations of Computer Science. 1985: 383-395.

Feldman（1987） 基于 Shamir 秘密分享体制，实现了可验证秘密分享协议，使得份额持有者可以对份额进行验证，并判断秘密分发者是否正确的执行了分发算法。

FELDMAN P. A practical scheme for non-interactive verifiable secret sharing [C]//Annual Symposium on Foundations of Computer Science. 1987: 427-438.

Pedersen（1992）提出的VSS方案。Feldman和Pedersen的方案是非交互的，因为分发协议不需要分发者和参与者之间或参与者之间的任何交互，除了提出投诉外。

Pedersen, T.P. (1992). “Non-interactive and information-theoretic secure verifiable secret sharing.” Advances in Cryptology—CRYPTO'91, Lecture Notes in Computer Science, vol. 576, ed. J. Feigenbaum. Springer-Verlag, Berlin, 129–140.

Jia等人（2019）和Verma等人（2020）基于中国剩余理论构造了 VSS 方案。

JIA X, SONG Y, WANG D, et al. A collaborative secret sharing scheme based on the chinese remainder theorem[J]. Mathematical Biosciences and Engineering, 2019, 16(3): 1280-1299.

VERMA O P, JAIN N, PAL S. A hybrid-based verifiable secret sharing scheme using chinese remainder theorem[J]. Arabian Journal for Science and Engineering, 2020, 45(4): 2395-2406.

Kandar 等人（2020）构造了一个 VSS 协议，该协议用一个新角色——组合器，从而可以识别恶意份额持有者的身份。

KANDAR S, DHARA B. A verifiable secret sharing scheme with combiner verification and cheater identification[J]. Journal of Information Security and Applications, 2020, 51: 102430.

3.公开可验证秘密共享（PVSS）

在可验证秘密分享 VSS 中，虽然份额可以被验证是否正确，但是对于公开的分布式协议来说，仅仅让协议内的参与者做验证是不够的。

Stadler（1996）基于VSS协议和离散对数问题，提出了公开可验证秘密分享(PVSS)协议，它通过对 VSS 协议中的份额进行加密保护，从而实现允许任何第三方对秘密份额的验证。

STADLER M. Publicly verifiable secret sharing[C]//International Conference on the Theory and Applications of Cryptographic Techniques. 1996: 190-199.

Fujisaki等人（1998）、Schoenmakers（1999）和Ruiz等人（2005）分别使用RSA算法、ElGamal密码和Paillier密码系统对份额加密，然后构建了各自的PVSS协议。

FUJISAKI E, OKAMOTO T. A practical and provably secure scheme for publicly verifiable secret sharing and its applications[C]//International Conference on the Theory and Applications of Cryptographic Techniques. 1998: 32-46.

SCHOENMAKERS B. A simple publicly verifiable secret sharing scheme and its application to electronic[C]//Annual International Cryptology Conference. 1999: 148-164.

RUIZ A, VILLAR J. Publicly verfiable secret sharing from paillier’s cryptosystem[C]//Western European Workshop on Research in Cryptology. 2005: 98-108.

Heidarvand等人（2009）基于双线性配对操作实现了一种新的PVSS协议。

HEIDARVAND S, VILLAR J. Public verifiability from pairings in secret sharing schemes[C]//Selected Areas in Cryptography. 2008: 294-308.

Jhanwar等人（2014）通过降低分发和重建阶段的计算成本，改进了Ruiz等人的协议（2005）。

JHANWAR M P, VENKATESWARLU A, SAFAVI-NAINI R. Paillier-based publicly verifiable (non-interactive) secret sharing[J]. Designs, Codes and Cryptography, 2014, 73: 529-546.

RUIZ A, VILLAR J. Publicly verfiable secret sharing from paillier’s cryptosystem[C]//Western European Workshop on Research in Cryptology. 2005: 98-108.

David 等人（2017）使用Reed-Solomon纠错码进一步提出验证复杂度更低的PVSS协议。

CASCUDO I, DAVID B. Scrape: Scalable randomness attested by public entities [C]//International Conference on Applied Cryptography and Network Security. 2017: 537-556

相对于 Schoenmakers 等人的方案，Janbaz等人（2020）和Zaghian等人（2020）进一步做出优化分发过程计算复杂度的PVSS研究。

JANBAZ S, ASGHARI R, BAGHERPOUR B, et al. A fast non-interactive publicly verifiable secret sharing scheme[C]//International ISC Conference on Information Security and Cryptology. 2020: 7-13.

ZAGHIAN A, BAGHERPOUR B. A fast publicly verifiable secret sharing scheme using non-homogeneous linear recursions[J]. The ISC International Journal of Information Security, 2020, 12(2): 91-99.

Gentry等人（2022）提出对数千个参与方的非交互式PVSS协议，其中底层的加密方案基于LWE问题，使用以下两个节省带宽的技术：对多接受者对情况采用Peikert-Vaikuntanathan-Waters(PVW)加密方案，同时在一个约256比特的DL-群上使用bulletproofs来获得正确加/解密份额的紧凑证明。

Gentry, C., Halevi, S., Lyubashevsky, V. (2022). Practical Non-interactive Publicly Verifiable Secret Sharing with Thousands of Parties. In: Dunkelman, O., Dziembowski, S. (eds) Advances in Cryptology – EUROCRYPT 2022. EUROCRYPT 2022. Lecture Notes in Computer Science, vol 13275. Springer, Cham. https://doi.org/10.1007/978-3-031-06944-4\_16