3 文献[11]的方案及其分析

本节对文献[11]构造的方案进行了具体的描述, 并对其方案的不满足方案所定义的 t-安全性的原因进行了具体的分析.

3.1 文献[11]的方案

为了解决现有 FSS 方案不具有门限的问题, 文献[11]给出了秘密函数为 $f_{a,b}(x):\{0,1\}^l\to GF_q$, n为参与者的个数, $t(t=l+1,t<n)$为重构门限的 FSS 方案在其方案中发送者 D 将$a\in\{0,1\}^l$转换为二进制表示, 则$a=(a_1,\cdots,a_l)$, 令$b=\prod_{j=1}^{l}b_j$, 其中$b_j\in GF_q$. 发送者 D 从GF_q中随机均匀地选取l个值$r_1,\cdots,r_l$, 生成$2l$个关于 z 的一次多项式$\begin{cases} g_j(z)=(r_j\cdot z+a_j)\cdot b_j \\ \hat{g}_j(z)=(1-(r_j\cdot z+a_j))\cdot b_j \end{cases}$. 之后 D 使用公开值$z_1,\cdots,z_n$计算$g_{j,i}=g_j(z_i),\hat{g}_{j,i}=\hat{g}_j(z_i)(i=1,\cdots,n)$, 并生成$k_i=(g_{1,i},\cdots,g_{l,i};\hat{g}_{1,i},\cdots,\hat{g}_{l,i})$. 之后 D 将生成的k_i发送给参与者P_i. 参与者P_i收到$k_i=(g_{1,i},\cdots,g_{l,i};\hat{g}_{1,i},\cdots,\hat{g}_{l,i})$后, 对于任意的$x_0\in\{0,1\}^l$, 将$x_0$用二进制表示为$x_0=(x_1^0,\cdots,x_l^0)$. 并计算$y_i=\prod_{j=1}^{l}(x_j^0\cdot g_{j,i}+(1-x_j^0)(1-\hat{g}_{j,i}))$. 在重构阶段任意 t 个参与者$P_{i_u}(u=1,\cdots,t)$通过$y=\sum_{u=1}^{t}c_{i_u}\cdot y_{i_u}$计算出秘密函数$f_{a,b}$在$x_0$点处的函数值, 其中, $c_{i_u}=\prod_{u'=1,u'\neq u}^{t}\frac{-z_{i_{u'}}}{z_{i_u}-z_{i_{u'}}}$.

正确性: 在文献[11]方案中存在关于 z 的 l 次多项式$f(z)=\prod_{j=1}^{l}(x_j^0\cdot g_j(z)+(1-x_j^0)(1-\hat{g}_j(z)))$,其常数项$f(0)=\prod_{j=1}^{l}(x_j^0\cdot a_j\cdot b_j+(1-x_j^0)(1-a_j\cdot b_j))$,对于任意的$x_0\in\{0,1\}^l$, 若$x_0\neq a$, 则存在$x_j^0\neq a_j$, 因此有$f(0)=0$. 若$x_0=a$, 则对任意的$(j=1,\cdots,l)$都有$x_j^0=a_j$, 因此有$f(0)=\prod_{j}^{l}b_j=b$. 所以$f(0)=\begin{cases}0,x_0\neq a\\ b,x_0=a\end{cases}$, 因此关于$z$的$l$次多项式$f(z)$的常数项$f(0)=f_{a,b}(x_0)$. 而每个参与者$P_i$通过$k_i(i=1,\cdots,n)$计算的值$y_i=\prod_{j=1}^{l}(x_j^0\cdot g_{j,i}+(1-x_j^0)(1-\hat{g}_{j,i}))=f(z_j)$. 因此任意$t(t=l+1,t<n)$个参与者可以通过多项式插值计算出$f(0)$, 进而重构出秘密函数$f_{a,b}$在点$x_0$处的函数值.

通过分析发现文献[11]的方案在保证方案正确重构的前提下, 其方案可以容忍$n-t$个参与者不参与重, 因此其方案可以更加灵活地应用到现实场景.

3.2 安全性分析

本小节对文献[11]方案的安全性进行分析. 详细分析了每个参与者如何通过自己的子函数来计算得到秘密函数$f_{a,b}$中 b 的值, 以及任意两个参与者联合如何计算得到整个秘密函数$f_{a,b}$, 具体过程如下:

1) 参与者$P_i(i=1,\cdots,n)$, 通过k_i计算秘密函数$f_{a,b}$中 b 的值.

在文献[11]的方案中 $k_i=(g_{1,i},\cdots,g_{l,i};\hat{g}_{1,i},\cdots,\hat{g}_{l,i})$, 其中 $g_{j,i}=g_j(z_i)=(r_j\cdot z_i+a_j)\cdot b_j$, $\hat{g}_{j,i}=\hat{g}_j(z_i)=(1-(r_j\cdot z_i+a_j))\cdot b_j$, 任意的参与者$P_i$计算$b_j=g_{j,i}+\hat{g}_{j,i}(j=1,\cdots,l)$, 从而得到$b=\prod_{j=1}^{l}b_j$.

2) 任意两个参与者 (不妨设为P_1,P_2) 联合通过k_1,k_2计算出秘密函数$f_{a,b}$.

参与者P_1收到子函数$k_1=(g_{1,1},\cdots,g_{l,1};\hat{g}_{1,1},\cdots,\hat{g}_{l,1})$, 参与者$P_2$收到子函数$k_2=(g_{1,2},\cdots,g_{l,2};\hat{g}_{1,2},\cdots,\hat{g}_{l,2})$, 由 1) 中的分析可知, 参与者$P_1$, P_2分别通过子函数k_1, k_2计算出$b_j(j=1,\cdots,l)$. 此时参与者P_1利用计算得到的b_j, 子函数k_1, k_2和公开值z_1, z_2计算$r_j=\frac{g_{j,2}-g_{j,1}}{b_j(z_2-z_1)}$, 同样参与者$P_2$利用计算得到的$b_j$, 子函数$k_1$, k_2和公开值z_1, z_2计算$r_j=\frac{g_{j,2}-g_{j,1}}{b_j(z_2-z_1)}$, 随后$P_1$计算$a_j=\frac{g_{j,1}}{b_j}-r_jz_1$. P_2计算$a_j=\frac{g_{j,2}}{b_j}-r_jz_2$. 此时参与者$P_1$, P_2可以分别独自计算出$a=(a_1,\cdots,a_l)$.

基于上述分析可知, 在文献[11]方案中任意两个参与者联合可以通过子函数和公开值计算出a, b的值, 从而得到秘密函数$f_{a,b}$且任意参与者可以通过子函数计算得到秘密函数$f_{a,b}$中 b 的值. 所以其方案不能抵抗 t 个参与者的联合, 因此不满足 FSS 方案中所定义的 t-安全性.

3.3 通信复杂度分析

在文献[11]的方案中$k_i=(g_{1,i},\cdots,g_{l,i};\hat{g}_{1,i},\cdots,\hat{g}_{l,i})(i=1,\cdots,n)$, 其$g_{j,i}=g_j(z_i),\hat{g}_{j,i}=\hat{g}_j(z_i)\in GF_q$, 因此$|k_i|=2l\cdot\log_2^q$. 因为 $y_i\in F_q$, 则$|y_i|=\log_2^q$. 因此$\Psi=\sum_{i=1}^{n}|k_i|+\sum_{u=1}^{t}|y_{i_u}|=(2nl+t)\cdot\log_2^q$. 因为$(n,t,\log_2^q)$为常数, 则$\Psi=O(l)$.

4 TFSS 方案与现有 FSS 方案的比较

本节我们将本文构造的基于多项式插值的门限函数秘密分享 TFSS 方案与现存的文献[5,6,9,11]中的

FSS 方案在方案所基于的工具, 有无门限值特性, 方案的安全性的级别以及方案的通信复杂度 4 个方面进行全面的比较. 为了比较的方便, 假设所有 FSS 方案分享的秘密函数均为点函数$f_{a,b}(x):\{0,1\}^l \to GF_q$, λ表示伪随机生成器种子的长度, t 表示重构门限值, n 表示参与者的个数. 具体比较结果见表 1.

表 1 TFSS 方案与现有 FSS 方案的比较

方案	基于的工具	(门限值, 参与者个数)	安全性	通信复杂度
文献[5]	伪随机生成器	(2,2)	计算意义下 t-安全	$O(\lambda l^{\log_2^3})$
文献[6]	伪随机生成器	(2,2)	计算意义下 t-安全	$O(\lambda l)$
文献[6]	伪随机生成器	(n,n)	计算意义下 t-安全	$O(\lambda 2^{(l+n-1)/2})$
文献[9]	伪随机生成器	(2,2)	计算意义下 t-安全	$O(\lambda l)$
文献[11]	多项式	(t,n)	无安全性	$O(l)$
TFSS	多项式	(r,n)	信息论意义下 t-安全	$O(l)$

经过比较发现本文构造的 TFSS 方案相对于文献[5,6,9]中构造的 FSS 方案具有额外的门限特性, 即在重构的过程中可以容忍参$(n-r)$个参与者不参与, 因此可以更加灵活地应用于现实场景, 且在安全性级别上由 2.2 节中对 TFSS 方案的安全性证明可得其为信息论意义下t-安全的, 而文献[5,6,9]中构造的 FSS 方案构造均基于伪随机生成器, 所以其方案的安全性基于密码学中单向函数的存在性假设, 进而为计算意义下t-安全的. 因此 TFSS 方案相对于文献[5,6,9]中构造的 FSS 方案具有更高级别的安全性. 此外在分享的秘密函数均为$f_{a,b}(x):\{0,1\}^l \to GF_q$的前提下, 由 2.3 节对 TFSS 方案的通信复杂的分析可得, TFSS 方案的通信复杂度为$O(l)$, 低于文献[5,6,9]中构造的 FSS 方案的通信复杂度. 在与文献[11]中构造的 FSS 方案对比中可以发现, 虽然 TFSS 方案与文献[11]中构造的 FSS 方案均具有门限的特性, 且具有相同级别的通信复杂度. 但在安全性上经过 3.3 节对文献[11]中构造的 FSS 方案的安全性分析可得, 其方案不具有 FSS 方案定义的 t-安全性, 而本文构造的 TFSS 方案具有信息论意义下 t-安全性.

5 结语

本文针对现有的函数秘密分享方在重构阶段需要所有参与者参与不能灵活的适用于现实场景的问题, 采用多项式技术构造了门限函数秘密分享方案. 并按照函数秘密分享方案定义的安全模型证明了新构造的门限函数秘密分享方案为信息论意义下安全的. 并对文献[11]构造了门限函数秘密分享方案进行的分析, 指出了其方案存在安全性漏洞. 最后本文将新构造的门限函数秘密分享方案与现有的函数秘密分享方案进行了比较, 发现其具有更高级别的安全性和更高的效率. 但事实上, 本文构造的门限函数秘密分享方案的门限值 r 是受限的, 要求$r=2lt+1$. 因此在未来是否能构造出门限值自由的函数秘密分享方案是一个值得继续思考的问题.

参考文献

1 Shamir A. How to share a secret. Communications of the ACM, 1979, 22(11): 612–613. [doi: 10.1145/359168.359176]

2 Blakley GR. Safeguarding cryptographic keys. Proceedings of the AFIPS 1979 National Computer Conference. Montvale, NJ, USA. 1979. 313–317.

3 Chor B, Kushilevitz E, Goldreich O, *et al*. Private information retrieval. Journal of the ACM, 1998, 45(6): 965–981. [doi: 10.1145/293347.293350]

4 Ostrovsky R, Shoup V. Private information storage (extended abstract). Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing. New York, NY, USA. 1997. 294–303. [doi: 10.1145/258533.258606]

5 Gilboa N, Ishai Y. Distributed point functions and their applications. Proceedings of the 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques. Copenhagen, Denmark. 2014. 640–658. [doi: 10.1007/978-3-642-55220-5_35]

6 Boyle E, Gilboa N, Ishai Y. Function secret sharing. Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Sofia, Bulgaria. 2015. 337–367. [doi: 10.1007/978-3-662-46803-6_12]

7 Boyle E, Couteau G, Gilboa N, *et al*. Homomorphic secret sharing: Optimizations and applications. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. Dallas, TX, USA. 2017. 2105–2122. [doi: 10.1145/3133956.3134107]

8 Plantard T, Susilo W, Zhang ZF. Fully homomorphic encryption using hidden ideal lattice. IEEE Transactions on Information Forensics and Security, 2013, 8(12): 2127–2137. [doi: 10.1109/TIFS.2013.2287732]

9 Boyle E, Gilboa N, Ishai Y. Function secret sharing: Improvements and extensions. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria. 2016. 1292–1303. [doi: 10.1145/2976749.2978429]

10 Håstad J, Impagliazzo R, Levin LA, *et al*. A pseudorandom generator from any one-way function. SIAM Journal on Computing, 1999, 28(4): 1364–1396. [doi: 10.1137/S0097539793244708]

11 Yuan DZ, He MX, Zeng SK, *et al*. (*t*, *p*)-threshold point function secret sharing scheme based on polynomial interpolation and its application. Proceedings of 2016 IEEE/ACM 9th International Conference on Utility and Cloud Computing. Shanghai, China. 2016. 269–275. [doi: 10.1145/2996890.3007871.]

12 Bellare M. A note on negligible functions. Journal of Cryptology, 2002, 15(4): 271–284. [doi: 10.1007/s00145-002-0116-x]