講演番号：31

盗聴と結託攻撃を考慮した関数分散に対する安全な協調再生成符号

A－2　Secure Cooperative Regenerating Codes for Distributed Function Against Eavesdropping and Collusion Attack

田中　洋輔†　栗原　正純†
Yosuke TANAKA†　Masazumi KURIHARA†
† 電気通信大学大学院　情報理工学研究科　情報・ネットワーク工学専攻
† Faculty of Informatics and Engineering, The University of Electro-Communications

1. はじめに

再生成符号は，分散ストレージシステムにおける次のような機能をもつ符号である[1]．k個の情報シンボルをn個の分散データに分散符号化し，それぞれをネットワーク上のn個のノードに保存する．このとき，任意のk個の分散データから元の情報を復元する機能と，ノード故障により消失した分散データをd個の故障していないノードからの修復用データから効率よく修復する機能を有する．さらに，t個の故障ノードを同時に修復可能な協調再生成符号の研究も行われている[2]．そして，秘密分散に基づく安全な(協調)再生成符号の研究も行われている[3]．一方，鍵配布に用いる関数分散に対応する再生成符号が提案されているが，そこでは安全性についての議論はなされていない[4]．また，関数分散に対応する協調再生符号，およびその安全性についても議論した研究はまだなされていない．そこで，本研究では盗聴とユーザの結託攻撃に対して安全な関数分散に対応する協調再生成符号を提案する．

2. メッセージの分散符号化

秘密分散に対する協調再生成符号[3]を関数分散に対する協調再生成符号に拡張することで提案符号は得られる．そのため，メッセージ行列や分散符号化，そして，修復に関する概要は，まったく同じではないが，文献[3]に従う．

メッセージ行列を，有限体F_q^N上の一様乱数で，かつ互いに独立な要素を成分とする$d \times (d+t)$行列$\underline{M} = \begin{bmatrix} \underline{R_1} & \underline{R_2} & \underline{R_3} \\ \underline{R_4} & \underline{S_1} & \underline{S_2} \\ \underline{R_5} & \underline{S_3} & \underline{O} \end{bmatrix}$と定義する．ここで，対角成分の部分行列$\underline{R_1}$, $\underline{S_1}$, $\underline{O}$はそれぞれ$l \times l$行列，$(k-l) \times (k-l)$行列，$(d-k) \times (d+t-k)$行列とする．$\underline{S_1}$, $\underline{S_2}$, $\underline{S_3}$を秘密情報とし，$\underline{O}$を零行列とする．

各$i = 1, \dots, n$に対し，F_q上の長さdと$d+t$のベクトルψ_iとϕ_iをノードiに付随する符号化ベクトルとする．それぞれの符号化ベクトルを並べた行列は Vandermonde 行列や Cauchy 行列となるものと仮定する．このとき，$(\psi_i^t \otimes I_N)\underline{M}$と$\underline{M}\phi_i$をノード$i$に保存する分散データとする．ただし，$I_N$は$N$次単位行列で，記号⊗はクロネッカー積を表す．

3. 各ユーザの関数値の復元と修復

各$j = 1, \dots, L$に対し，ユーザjは，自身の ID $\underline{x_j} \in F_q^N$に対する関数値$F(\underline{x_j}) = (I_d \otimes \underline{x_j}^t)\underline{M}$を鍵として知りたい．そこで，ユーザは，任意の$k$個のノードに自身の ID を送信する．すると，各ノードiは自身が保存する分散データを用い，$\underline{x_j}^t(\psi_i^t \otimes I_N)\underline{M}$と$(I_d \otimes \underline{x_j}^t)\underline{M}\phi_i$を計算し，その値をユーザに送り返す．このとき，ユーザjはk個のノードから集めたデータより所望の関数値を復元することができる．ただし，$N \leq L$であり，ID のベクトルを並べた行列は Vandermonde 行列や Cauchy 行列となるものと仮定する．

一方，修復については，t個の故障ノードを協調して同時に修復を行うことを考える．故障ノードおよびそれに対応する新しく置き換えられる置換ノードを簡便に同じfと表す．置換ノードfは故障していないd個のノードにアクセスする．各ノードiは自身が保存している分散データから$(\psi_i^t \otimes I_N)\underline{M}\phi_f$と$(\psi_f^t \otimes I_N)\underline{M}\phi_i$を計算し，置換ノード$f$へ送る．次に，置換ノード$f$は集めたデータから$(\psi_f^t \otimes I_N)\underline{M}\phi_f$を計算し，自身を除いた$t-1$個の他の置換ノードに送信する．これらの修復用データを集めた置換ノードは，故障ノードが保存していた分散データ$(\psi_f^t \otimes I_N)\underline{M}$と$\underline{M}\phi_f$を修復できる．

4. まとめ

前記までの設定により，以下の安全性をもつ安全な協調再生成符号が得られる．

(1) 盗聴により，l個以下の分散データが漏洩しても，それらから秘密情報に関する情報は得られない．
(2) 結託により，$N-1$人以下のユーザの関数値が集められても，それらから秘密情報に関する情報は得られない．

参考文献

[1] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," *IEEE Trans. Inf. Theory,* vol. 56, no. 9, pp. 4539-4551, Sep. 2010.
[2] A. Wang and Z. Zhang, "Exact cooperative regenerating codes with minimum-repair-bandwidth for distributed strage," Proc. *IEEE INFO-COM*, pp. 400-404, Apr. 2013.
[3] O. O. Koyluoglu, A. S. Rawat, and S. Vishwanath, "Secure Cooperative Regenerating Codes for Distributed Strage Systems," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5228-5244, Sep. 2014.
[4] 吉田隆弘，地主創，"関数に対する最小バンドワイド再生成符号に関する一検討，" Proc. SITA2012, pp.61-66, Dec. 2012.