秘密計算の概念はそろそろ統一した方がよくない?

五十嵐 大[1,a)]

概要：秘密計算には主に Yao の Garbled Circuit, 準同型暗号, 秘密分散ベース秘密計算がある. しかしこれらの性質は別々に論じられており, 統一的に扱う議論は無かった. 本稿ではこの課題を解決すべく筆者の意見を述べる.

キーワード：秘密計算, Girbled Circuit, 準同型暗号, 秘密分散

By Now, Isn't It Better to Unify Notions of Secure Computation Methods?

Dai IKARASHI[1,a)]

Abstract: Secure computation technology mainly involves Yao's Garbled Circuit, Homomorphic Encryption and Secret-sharing-based Multi-party Computation. However, there are no discussion to unify them. In this paper, I state my opinion to solve this problem.

1. はじめに

秘密計算は暗号化したまま処理が可能な暗号技術であり, 複数者のデータを秘匿したまま集約して処理をする統合データ分析などの有望な応用が考えられている. 秘密計算は性能が課題であったが近年目覚ましい性能向上を遂げており, AI などの先端的な処理も現実的となりつつある.

しかし秘密計算を普及させてゆくときに, 主に Yao の Garbled Circuit[1], 準同型暗号, 秘密分散ベース秘密計算, であるが, どうしても方式ごとに性質, 特に安全性の比較をしてしまい, "この方式でなければだめだ" という結論に落ち着きがちである. しかし理解しておきたいのは, **いずれの秘密計算でも平文で処理するより安全であるという当たり前の事実**である. 理想を目指すために, 我々は一足飛びではなく, 次のステップへ進むことを繰り返すべきである.

本稿は技術的に深い議論ではないし, 述べたいことは全然多くはない. しかし述べておかねばならない. なお筆者は秘密分散ベースの秘密計算を直近では推しているが, 性能の観点だけの話だし, 他の方式も研究していたし今もある程度はしている, そういう者である.

[1] NTT セキュアプラットフォーム研究所, NTT Secure Platform Laboratories
[a)] dai.ikarashi.rd@hco.ntt.co.jp

2. "暗号" と "秘密分散"

困難の一端は, "暗号" と "秘密分散" が統一的に扱われていないことだと考えられる. なぜなら, 秘密計算の安全性はそれらの方式の上に成り立っているからである.

まず筆者の主張は, 秘密分散は暗号の一種である, ということである.

(1) よく知られるバーナム暗号は秘密分散である.
(2) そもそも一般の人にとって, (筆者の経験上) 暗号と画像・音声符号化の区別もついていないのに暗号と秘密分散を異なる技術と捉える必然性はない

技術的には, 暗号とは "鍵がなければ暗号文が解読できない (逆もまた然り)", 秘密分散とは "所定個以上のシェアを集めなければ復元できない (逆もまた然り)" である. この意味では, サイズの制限を設けなければ, 鍵と暗号文をシェアとして暗号を $(2,2)$-秘密分散と見なせるから, 秘密分散がより広い集合である. 一方で, 秘密分散のシェアを鍵と見なせば秘密分散は暗号である. すなわち, 抽象的な意味では**論理的に暗号と秘密分散は同値である. つまり, どっちがどっちでもいいのである.**

暗号学者のいわゆる "暗号" と "秘密分散" は, 暗号とは

暗に計算量的安全性をもち鍵が暗号文に対して無視できるサイズの可搬性を実現した便利な道具である. しかし Krawczyk の発明 [2] により秘密分散も計算量的安全性を持ちシェアサイズを自由にできるため, この境界ももはや曖昧である.

3. 準同型暗号は 1 パーティなのか

前節と同じことを別の言い方で言うようなものだが, 準同型暗号は 1 パーティで計算できるのが良いところである. と言われる. しかしそれはあくまで, 鍵のことを気にしない前提である. 実際には計算結果を得るときに復号という計算が必要である. **復号を計算に含めないのは一般人の感覚からしたらよく分からない話である.** そして鍵管理も必要である. 鍵管理はセキュリティ業界では重要な課題であり, 理論的には守られている前提で良いが, 現実的な安全性としてはやはり鍵と暗号文をしっかり分けることである. **暗号学者が "計算" と見なす処理が 1 パーティにあるのかどうかは, 性能面でネットワークに依存するかどうかなのであり, 安全性に関しては関係の無い話である.**

4. "結託" とは何なのか

これも同じ話なのであるが, 秘密分散は結託に弱いとよく言われる. しかしここまでの議論を踏まえると, 暗号も鍵と暗号文が集まると復号できるので, 結託に弱いのは秘密分散だけの性質ではない.

5. 情報理論的安全性?

情報理論的安全性とは秘密分散の基本的な安全性で, 計算量的安全性よりも強い. しかし, 筆者は暗号学者の端くれなので, **計算量的安全性は十分な安全性だと考えている.** 特段の理由がない限り, 情報理論的安全性を追い求める必要はないであろう. 情報理論的安全性に関しても, 秘密計算では安全性以外のメリットがある (間接的には安全性だが). それは, アルゴリズムが特定の暗号方式に依存しなくなる, という点である. 情報理論的安全であっても通信路等で結局計算量的安全の暗号を使うことが普通であるが, 秘密計算アルゴリズムと計算量的安全な暗号が分離され, 危殆化が発生してもアルゴリズムは変更が不要で, 更改が容易となる.

6. malicious?

semi-honest (passive) は盗み見のみする攻撃者の前提, malicious (active) は積極的攻撃 (改ざん) を行う攻撃者の前提である. malicious の方が強い安全性である. しかし世の中で承認さられている暗号は, 改ざんに対応する暗号だけであろうか. **実際は改ざんに対抗しない暗号も普通に認められている.** 何が何でも malicious でなければならない, というのは過剰反応である.

7. dishonest-majority?

dishonest-majority とは, 攻撃者側のパーティが半数以上であることである. これも理想的だが, リスク工学で分かっていることは, 単位時間内に安全性が破られる確率は秘密分散で言えば k, すなわち許容される攻撃パーティ数にほぼ依存するということである. 別に honest-majority だろうが dishonest-majority だろうが, 本当は k が大きいかどうかしか問題ではない. そして, 通常使われる "暗号" は $k = 2$ と, この意味では最低値である. **すなわち, Yao でも準同型暗号でも $(2, 3)$-秘密分散ベースでも, "暗号" 程度の安全性は持っているのである.**

8. おわりに

言いたいことは今のところこれくらいである.

秘密計算の概念を統一して暗号学者以外に秘密計算をよく理解してもらうため, 幾つか言いたいことを言った. 要約すると, 実際はどの方式も安全なので, 過度の学術的比較を暗号学者以外の方々に披露することは理解が遠のくだけである.

参考文献

[1] Yao, A. C.-C.: Protocols for Secure Computations (Extended Abstract), *FOCS*, IEEE Computer Society, pp. 160–164 (1982).

[2] Krawczyk, H.: Secret Sharing Made Short, *Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings* (Stinson, D. R., ed.), Lecture Notes in Computer Science, Vol. 773, Springer, pp. 136–146 (online), DOI: 10.1007/3-540-48329-2_12 (1993).