博士後期課程

博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

論文題目　：　Research on Fast Hierarchical Secret Sharing Schemes
申請者　：　島 幸司
審査委員会　：　主査　教授　土井 洋
副査　教授　有田 正剛
副査　教授　大塚 玲
副査　教授　大久保 隆夫

Ⅰ．論文内容の要旨

本論文は“Research on Fast Hierarchical Secret Sharing Schemes (高速な階層的秘密分散法の研究)”と題し、8 章からなっている。

第 1 章“Introduction”では、本論文の研究背景や課題について述べている。秘密情報の安全な保管は情報化社会において重要な課題である。この情報の盗難対策や紛失対策を同時に満たす方法として秘密分散法が知られている。(k,n)しきい値法では、秘密情報から n 個のシェアを生成し参加者に分散し、それらのうち任意の k 個のシェアを集めれば秘密情報を復元できる。一方 k 個未満のシェアからは秘密情報を復元できない。本論文で扱う階層的秘密分散法では参加者集合をレベルで分割することができる。例えば、金庫を開けるためには 3 人の従業員の協力が必要で、少なくとも 1 人は部長といったシナリオの場合は、$(\{1,3\},n)$階層的秘密分散法を用いることができる。このシナリオにおける部長は必須参加者とみなすことができるが、$(\{1,3\},n)$階層的秘密分散法を用いることで、分散管理された秘密情報の消去も容易になる。実際、必須参加者のシェアのみを削除することで、残りのシェアを用いても秘密情報は復元できなくなる。なお(k,n)しきい値法にはいくつかの高速化手法が存在するが、階層的秘密分散法の高速化手法が知られていないことを指摘している。以上を踏まえて、高速な階層的秘密分散法の構成法を複数示したことを説明している。なお、提案した構成法では参加者集合を複数のレベルで分割可能である。

第 2 章“Preliminaries”では、完全秘密分散法と理想的秘密分散法の定義に加え、本論文で扱う階層的秘密分散法を定義している。更に 3 章以降で必要となる事項を整理し、性能評価のための実験環境等を示している。

第 3 章“HSSS over Finite Fields of Characteristic Two”では、標数 2 の有限体上での階層的秘密分散法の構成方法を示している。標数が大きな素数の有限体上での構成方法として導関数と Birkhoff 補間法を利用する方法が知られていたが、これは標数 2 の有限体上には適用できない。そこで、導関数にかわる関数を新たに導入することで、標数 2 の有限体上での階層的秘密分散法の構成に成功したことを述べている。また、この構成方法は完全かつ理想的なものであることを示し、性能評価結果を示すとともに、性能向上等のためのいくつかの手法についても述べている。

第 4 章“HSSS Based on Information Dispersal Techniques”では、誤り訂正符号などと関係が深い情報分散アルゴリズム(IDA)を用いた構成方法を示している。IDA を用いた(k,n)しきい値法については 2016 年に提案されているが、このアイデアを元に階層的秘密分散法の構成に成功している。なお、この構成方法も完全かつ理想的なものである。

第 5 章“XOR-based HSSS for a Small Number of Indispensable Participants”では、XOR 演算のみで実現可能な$(\{1,3\},n)$階層的秘密分散法の構成方法を示している。この構成方法は、階層が$(\{1,3\},n)$に限定されるなどの制限があるが、分散管理された秘密情報の消去のような具体的なシナリオでは利用可能である。この構成方法も完全かつ理想的であり、処理性能が高速であることも示している。

第 6 章“XOR-based HSSS”では、XOR 演算のみで実現可能な階層的秘密分散法の構成に成功したことを述べている。この方法では、第 5 章で提案した方法において設けざるを得なかった階層の限定等の制限を解決している。これはシェア生成のために用いる行列の工夫により階層的秘密分散法を実現したものであり、完全かつ理想的な秘密分散法であることを示すとともに、性能評価結果を示している。

第 7 章“Computational Costs”では、第 3 章から第 6 章までの各構成方法の処理性能について整理し、構成方法毎の性能について分析し、議論している。その上で、階層構造のパラメータ、特に参加者総数nと構成方法の処理性能について述べている。

第 8 章“Conclusions”では、第 1 章で述べた課題に対して、4 つのアプローチからなる構成に成功したこと、そしてそれらの処理性能について要約している。

Ⅱ. 論文審査結果の要旨

本論文は、情報化社会において秘密情報の安全な保管、特に情報の盗難対策や紛失対策を同時に満たし、分散管理された秘密情報の消去も容易な階層的秘密分散法の高速な構成方法に対して、複数のアプローチから検討し、具体的な構成方法を示したものであって、情報学並びに情報社会の発展に貢献するところが大きい。よって、本論文は情報学における博士論文として十分価値のあるものと認める。

Ⅲ. 審査経過

本審査委員会は、平成 31 年 1 月 29 日に論文内容とこれに関連する事項について口述試問を行い、申請者が学位取得にふさわしい知見を持つものと判断した。

情報セキュリティ大学院大学　情報セキュリティ研究科