暗号技術の新展開

野島 良 (のじま りょう)
ネットワークセキュリティ研究所
セキュリティ基盤研究室 主任研究員

大学時代に暗号技術を試みましたが、全く歯が立ちませんでした。その延長線上に今の自分がいますが、今は暗号解読ではなく、暗号技術を設計する立場になりました。博士(工学)。

「盗聴者への情報漏えいを防ぐことを主目的として発展してきた暗号技術に対する新たな展開先、プライバシー確保型 IP トレースバックを紹介します。」

暗号技術の広がり

暗号技術は、2 者間の通信において盗聴者にメッセージの内容が漏れないようにすることを主目的として発展してきました。しかし、近年のインターネットの発展に伴い、その応用範囲は急激に拡大しています。その中でも、我々が所属するネットワークセキュリティ研究所においては、内積暗号、秘匿計算プロトコルと呼ばれる汎用性の高い暗号技術の研究・開発に力を注いできました。ここでは、秘匿計算プロトコルの一種である「オブリビアス秘密鍵暗号プロトコル」とその応用技術「プライバシー確保型 IP トレースバック」について紹介したいと考えています。

そもそも IP トレースバック技術とは、インターネット上で不正を働いたユーザを追跡する技術です。もう少し具体的に述べると、IP トレースバックにおいては、各ルータが通過するパケットを保存しておきます。そして、実際に攻撃が行われた際には、攻撃を行ったパケットが保存されているルータを探索することにより、結果的に攻撃を行ったコンピュータを見つけ出すことが可能となります。

この IP トレースバック技術は非常に有用な技術ですが、探索する際に不正ユーザだけではなく、正当なユーザのプライバシーをも暴露してしまう可能性があります。我々が提案したプライバシー確保型 IP トレースバック技術は、IP トレースバック技術の一種です。ただし、正当なユーザのプライバシーを確保しながら、不正ユーザを追跡することが可能になります。

IP トレースバックとプライバシー確保型 IP トレースバックに関する問題は、次のように単純化することができます。2 人のユーザ(花子と太郎)を考えます。太郎は IP アドレスの集合 $A=\{a_1, \cdots, a_n\}$ を、花子は IP アドレス a を保持しているとします。花子の目的は、A の中に a が含まれているかどうか調べる事です。この問題は、花子が a を太郎に送り、太郎が A の中に a が含まれているかどうかを調べる事により解決可能になります。実際に IP トレースバックでは、同じようなことが行われます。一方、プライバシー確保型の IP トレースバックにおいては、問題が若干難しくなります。この技術を実現するためには、太郎が A を漏らさずに、そして花子が a を漏らさずに、a が A に含まれているか調べることが必要になります。この一見解決不可能な問題を、我々は、オブリビアス秘密鍵暗号プロトコルを開発・応用することにより解決しました。ここでは、このオブリビアス秘密鍵暗号プロトコルの概要とその応用についてご紹介します。

秘密鍵暗号

秘密鍵暗号においては、秘密鍵 SK を使いメッセージ M を暗号化することができます。

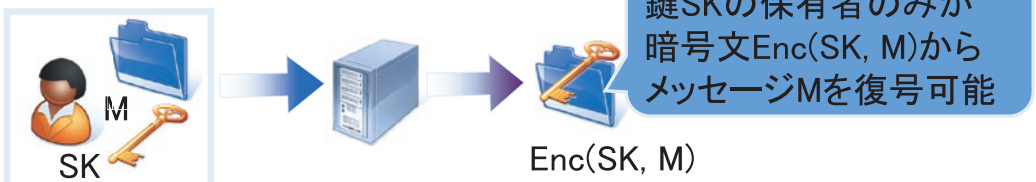

図1　秘密鍵暗号の説明

この暗号化されたメッセージを Enc(SK, M) と表します。ここで秘密鍵 SK を保有する人だけが、Enc(SK, M) から M を取り出すことが可能になります。逆に、SK を保有していない人は M に関する情報を一切得る事ができません(図 1)。秘密鍵暗号として代表的なものに、DES(Data Encryption Standard) と AES (Advanced Encryption Standard) があります。

オブリビアス秘密鍵暗号

オブリビアス秘密鍵暗号プロトコル(以降、OEP) は、2 者(太郎、花子) 間の暗号プロトコルです。

太郎は秘密鍵暗号の秘密鍵 SK を、花子はメッセージ M を保有します。このプロトコルは、お互いの情報 SK と M を秘密にしたまま暗号文 C = Enc(SK, M) を計算することを可能にします。ここで、もちろん C を得られるのは花子であり、太郎は C に関する情報を一切得る事ができません(図 2)。

ここで「オブリビアス」という単語に関してですが、直訳すると「気付かない」という意味があります。太郎と花子は相手の入力について「気付かない」ため、プロトコル名にオブリビアスという用語が使われています。

IP トレースバックへの応用

プライバシー確保型 IP トレースバック技術において、太郎と花子は、お互いの情報を隠しながら、a が $A = \{ a_1, \cdots, a_n \}$ に含まれているかどうかを検証する必要がありました。この問題は、OEP を使うと簡単に解決できます。

(1) 太郎は、秘密鍵暗号の秘密鍵 SK を選び、Enc(SK, a_1)、…、Enc(SK, a_n) を花子に送ります。

(2) 花子は、OEP を使い Enc(SK, a) を得ます。そして、Enc(SK, a_1)、…、Enc(SK, a_n) の中に、Enc(SK, a) と同じになるものがあった場合、a が A に含まれていると判定します。OEP を使うことにより、お互いに SK と a が漏れないため、花子の秘密情報である a が太郎に漏れる事はありません。さらに、SK が花子に漏れないので、n 個の暗号文から太郎の秘密情報 A が漏れることもありません(図 3)。

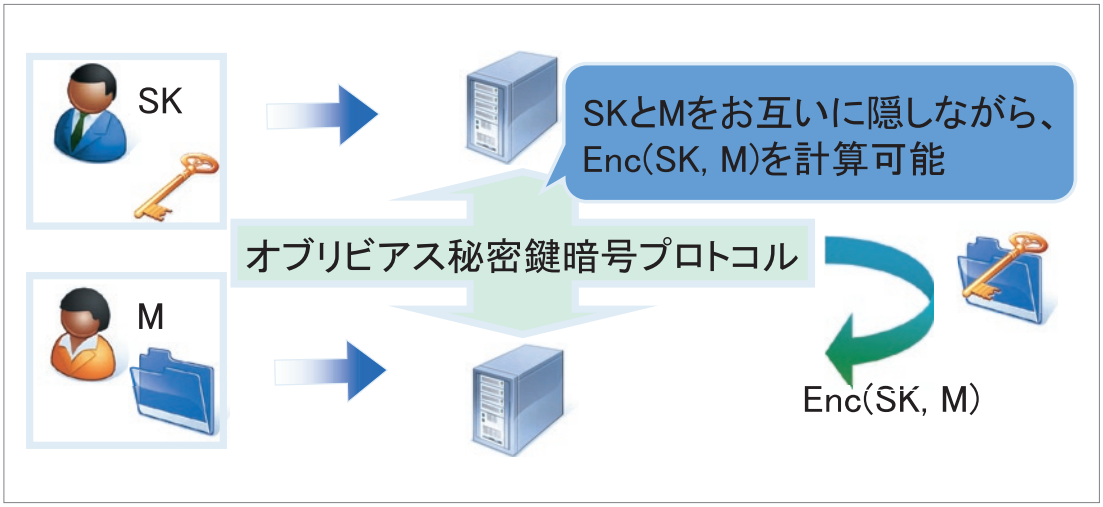

図2　オブリビアス秘密鍵暗号プロトコルの説明

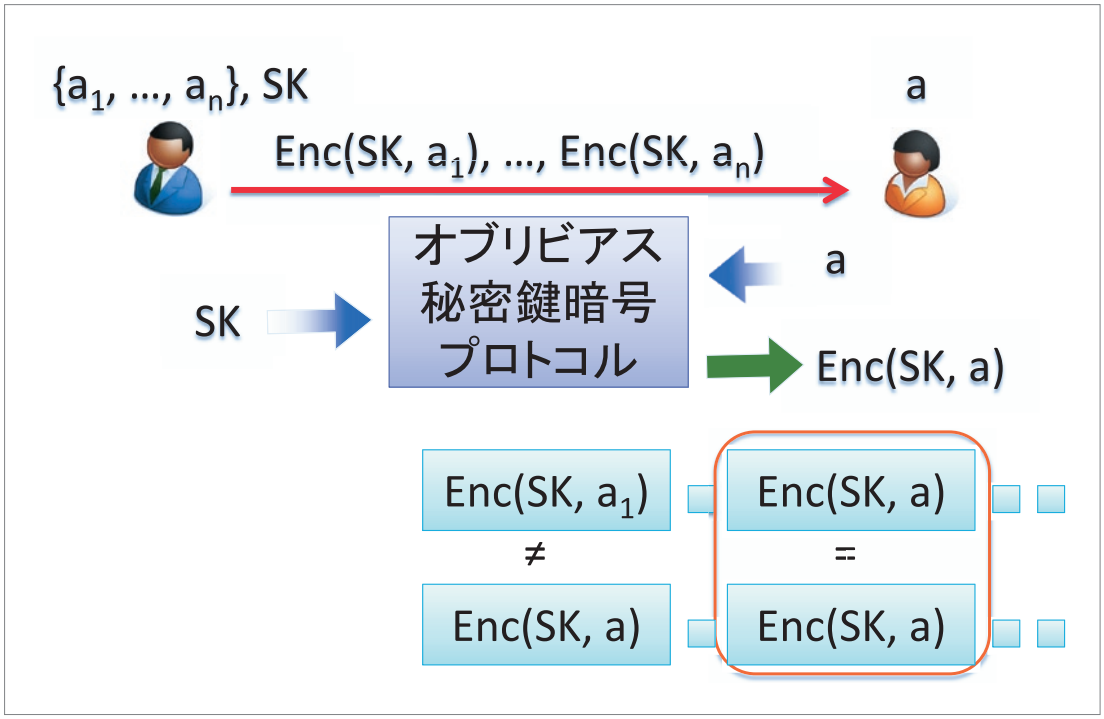

図3　プライバシー確保型IPトレースバックの説明

今後の研究について

ここまでオブリビアス秘密鍵暗号プロトコル、及びプライバシー確保型 IP トレースバック技術を簡単に紹介してきました。その具体的構造まで説明することはできませんでしたが、既にオブリビアス秘密鍵暗号プロトコルは、実装・実験が無事に終了しています。今後は、IP トレースバック技術、オブリビアス秘密鍵暗号の更なる発展・普及に努めたいと考えています。