可換型暗号を使った秘密の共有

Saied Hosseini

Khayat* 2008年8月18

日

概要

秘密を共有するために可換暗号化を使用する方法が示されている。アリスがボブと秘密を共有し、受託者のグループが同意しない限りボブがその秘密を復号できないようにしたいとする。アリス、ボブ、受託者は安全でないチャネルで通信すると仮定する。本論文では、モジュール指数を用い、鍵交換を必要としない方式を提案する。この方式の安全性は、離散対数問題の難しさに依存している。

キーワード：秘密分散、可換暗号。

1 はじめに

アリスがある秘密（例えば銀行のパスワード）を持っていて、それをボブと安全に共有し、ボブが受託者のグループの同意なしに秘密を解読できないようにしたいとします。さらに、以下の仮定を考える。

1. アリス、ボブ、受託者は、安全でない公開チャンネルでのみ通信できる。
2. その秘密は、評議員にも、ボブ以外の誰にも明かさないことだ。
3. 関係者は、定められたプロトコルに従うことで信頼できる。

上記の問題は、商業的、企業的、軍事的な環境で発生する可能性があり、（セクション4で説明する）Shamir threshold スキーム [4] などのよく知られた秘密共有スキームによって解決することができる。これらの方式では、秘密を解除するために、株主は自分たちの株を安全に「プール」しなければならない。当事者が遠隔地にいる場合、通常、プロトコルの実行前に鍵交換が必要である。分散型アプリケーションでは、秘密分散方式に先立つ安全な鍵配布の手間を省くことは、価値ある目標である。本論文では、モジュラー指数演算のような可換な暗号化関数を用いて、前述の問題を解決するキーレス方式を作成する方法を示す。この方式の安全性は、離散対数問題の難解さにかかっている。本論文は以下のように構成されている。第2節では、本論文のキーアイディアを説明する。第3節では、我々の提案する方式を示し、その正しさと安全性を示す。第4節では、提案方式の利点について議論し、最後に本論文の貢献度をまとめる。

*イラン、マシュハド、フェルドウィーシ大学電気工学部電子メール： *shk@alum.wustl.edu*

2 キー アイデア

本論文では、Shamirの鍵なし秘密通信[3, pp.500]にヒントを得て、モジュラーエキスポーネーションの可換特性を利用した秘密分散方式を提案する。しかし、このアイデアは、ある条件を満たした可換な暗号化関数であれば有効である。Shamirは[5]で、暗号における可換性の威力を探求しています。文献[1]と[2]はそれぞれ、データベース間の情報共有や、分散データマイニングにおけるプライバシーのために可換暗号方式を使用しています。このトピックは、[6]において、最近の基礎的な考察を多く受けている。

提案する方式では、可換性が重要な役割を果たします。可換性は、信頼された当事者が秘密を暗号化した後に、秘密の所有者が自分の暗号化を取り消すことを可能にします。また、信頼された当事者が、共有手続きを再開することなく、任意の順序でグループに参加したり離脱したりすることができる。

定義1 Mを*メッセージ空間*、Kを*鍵空間とする。***可換型暗号化***関数とは、任意の*$m \in$Mに対して、*任意の*a、$b \in$Kに対して、$f_a \circ f_b(m) = f_b \circ f_a(m)$ *となるような双射*$f: M \times K \rightarrow M$*の族である。*

ある条件の下でのモジュラー指数関数が可換な暗号化関数であることを示すのは簡単な練習です。

事実1 *素数*p*を固定し、*$f_a(m) \stackrel{\text{def}}{=} m^a \pmod p$*と定義する。* $m \in Z$ *と*$a \in Z$ *というような* gcd$(a, p-1) = 1$*とする。すると*

1ページ目

a) $f_a(m)$ *は双射である。証明する。*$f_b \circ f_a(m) = m$*となる*$b \in Z_{p-1}$ *が存在する。これは次のように簡単にわかる。*$a \in Z_{p-1}$、gcd$(a, p-1) = 1$*とすると、*$ab = 1 \pmod{p-1}$*となる*$b \in Z_{p-1}$ *（拡張ユークリッドアルゴリズムを用いて）を求めることができる。その結果*

$$f_b \circ f_a(m) = m^{ab} \pmod p = m^{1+k(p-1)} \pmod p = m,$$

ここで、フェルマーの定理（$m \in Z_p$*, then* $m^{(p-1)} = 1 \pmod p$*）を利用しました。*

b) $f_a(m)$*は可換である。証明する。すべての正の整数*a,b,m*に対して*

$$f_a \circ f_b(m) = m^{ab} \pmod p = f_b \circ f_a(m)$$ です。

上記の事実は、我々の鍵なし秘密分散方式が正しいことを示す鍵である。

3 提案されたスキーム

3.1 商品説明

提案するアルゴリズムは、大きな素数pが全ての人に（敵対者にも）公知であるとの仮定を用いる。この素数は、この種のアプリケーションの技術標準の一部とされ、その後、世界に公開されることができる。その結果、素数pは認証された形で誰もがアクセス可能であると仮定する。

以下では、便宜上、秘密の所有者(Alice)をP_0 で表す。 受託者は、$P_1, P_2, \ldots, P_{n-1}$ で表す。最後に、P_n は、秘密の受信者(Bob)を表す。また、"ロック "という言葉は、"暗号化 "とい

う意味で使っている。

我々のプロトコルは3つのフェーズを持つ。(1) 設定、(2) ロック、(3) 解除。各フェーズを以下に説明する。

設定する。 公開された大きな素数p。当事者P_0 が所有する秘密鍵$s \in Z_p$ 。各当事者P_i は、$i = 0, 1, \ldots, n$ に対して、$a_i, b_i \in Z_p$, $\gcd(a_i, p-1) = 1$, および $a_i b_i = 1 \pmod{p-1}$ の自分自身の秘密鍵ペア (a_i, b_i) を持っている。

ロックする。 このフェーズでは、すべての当事者によって、次のようにカスケード方式で秘密がロックされる。

1. 秘密の所有者であるP_0 (アリス)は、$c_0 = s^{a_0} \pmod{p}$とすることで秘密sをロックし、c_0 をP_1 に送る。
2. $i = 1, 2, \ldots, n-1$について、当事者P_i は、$c_i = c_{i-1}^{a_i} \pmod{p}$、および$c_{i-1}$ を行うことによって、秘密をロックする。
   は、秘密c_i をP_{i+1} に送信する。
3. P_n は、$c_n = c_{n-1}^{a_n} \pmod{p}$ とし、c_n を P_0 に送る。
   ロックする。
4. 秘密の所有者P_0 は、ここで自分のロックを秘密から取り除く。その結果、共有secret $s^l = c_n^{b_0} \pmod{p}$とする。彼女はs^l をP_n (Bob)に送信する。

ロック解除。 この段階では、まずすべての受託者（任意の順番で次々に）が秘密を解き、最後の段階でP_n が、次のようにして秘密を解き明かす。

1. P_n は $d_i = s^l$ とし、d_i を受託者 P_i , $i \in \{1, 2, \ldots, n-1\}$に送信する。
2. 各管財人P_i は、$\{P_1, P_2, \ldots, P_{n-1}\}$の中で、（任意の順序で）自分の持ち物を削除する。(任意の順序)で、自分の
   $d_i^{b_i} \pmod{p}$を行うことで共有秘密からロックし、その結果を
   次の受託者。$P_1, P_2, \ldots, P_{n-1}\}$の最後の受託者は、共有秘密から自分のロックを外し、その結果をP_n に送信する。
3. この時点で、P_n 、$s = d_n^{b_n} \pmod{p}$を行うことで秘密が解かれる。この時点ではボブ (P_n) は秘密を知る。

上記プロトコルの実行により、受託者グループの全会一致のもと、秘密が分散的に秘密所有者から第2者に譲渡される。

3.2 コレクトネス

この方式の正しさは、次のように、事実1を用いることで容易に立証することができる。ロックフェーズの終了時に、共有秘密 s^l は

$$s^l = s^{a_0 a_1 a_2 \cdots a_n b_0} \pmod{p} = s^{a_1 a_2 \cdots a_n} \pmod{p}$$です。

と、ロック解除の段階の最後にあります。

$$s^{l(b_1 b_2 \cdots b_n)} \pmod{p} = s^{(a_1 a_2 \cdots a_n)(b_1 b_2 \cdots b_n)} \pmod{p} = s \text{となります。}$$

このように、モジュラーエクスペリエンスの可換性により、ロック解除操作の順序は重要でない。最後の秘密sは、P_n によって得られる。

3.3 セキュリティ

本方式の安全性は、離散対数問題(DLP)の計算の難しさに依存する。敵対者は、本方式を破るために、以下のいずれかの目標を追求することができる。

- 完全に破たん。彼はその秘密を知ることで、全会一致の要件を完全に回避することができる。
- 部分的に破る。当事者の1人以上の秘密鍵(a_i または同等に b_i)を見つけ出す。これにより、彼はある受託者の役を演じ、彼らの同意する権利を盗むことができる。

以下の論証により、本方式の安全性を立証することができる。

a) 最初のロックホップ、$_{ip}P_0$ から P_1 において、秘密鍵の所有者は秘密鍵 s ($c_0 = s^{a_0} \bmod p$) をロックしてから P_1 に送る。敵対者は a_0 と s という二つの未知数を探索しなければならないことに 注意。敵対者は a_0 を知らなければ s を推測することができない。

b) その後のホップでは、敵はP_{i-1} から送信中のc_{i-1} を盗聴し、読み取ることができる。
P_i 、彼はP_i からP_{i+1} への転送中にc_i を読むことができる。 a_i を見つけるために、敵対者は以下を解かなければならない。
a DLP $(c_i = c^{a'}_{i-1} \bmod p)$であるが，これは実行不可能である．もし成功すれば、b_i を計算することができる。
共有秘密 s^l を解くために必要な鍵の一つである。
をすべてのホップに対して行い、すべてのb_i 'sを取得する。一方、敵対者がb_i 'sのいずれかを決定した場合、彼は対応する当事者の役割を果たし、秘密の不正な解除のために共謀することができる。DLPを解くことは計算上困難であるため、上記のような可能性は限りなくありえない。

c) 最後のロックホップでは、s^l がP_n に送信される。敵はこれでc_n とs^l を知ることができる。
を$_0$求めるために、DLP ($s^l = c_n^{b_0} \bmod p$) を解かなければならない。

e) ロック解除の段階でも、同じ種類の議論が有効である。共有秘密は、転送中に少なくとも1つの当事者によって常にロックされる。

f) 秘密鍵が偶然に以下のように選択される可能性はゼロではない。

$$a_0\, a_1 \equiv 1 \pmod{p-1}$$、または

$$a_0\, a_1\, a_2 \equiv 1 \pmod{p-1}$$, または

$$a_0\, a_1 \cdots a_n \equiv 1 \pmod{p-1}$$

この$_i$場合、秘密鍵sはP_i からP_{i+1} への転送中に漏洩する。 しかし、鍵を巨大な空間から選択しなければならないことを考えると、 上記のいずれの事象も発生する確率は無視できるほど小さい。

したがって、この方式の安全性は、冒頭で主張したように、DLPに依存することが示された。

4 ディスカッション

この方式には、いくつかのメリットがあります。

a) この方式では、プロトコルに先立って秘密鍵や公開鍵を交換する必要がない。これは本方式の主な利点である。そうでなければ、同じ目的（すなわち、グループの同意の

下での秘密の伝達）は、以下の方法で、Shamirのようなよく知られた秘密共有方式を用いて達成することができるからである。

アリスは秘密を利用して、被信託者の数と同じ数の株式を作成する。それから、彼女はすべての共有を同じ秘密鍵Kで暗号化し、 暗号化された共有を自分の被信託者に送る。彼女はまた、KをBobに送る。Bobが秘密を解く必要があるとき、そしてすべての受託者が同意したとき、受託者は暗号化された共有物をBobに送る。その後、彼はすべての共有を復号化し、関連するプーリングアルゴリズムを使用して秘密を計算する。

上記のプロトコルでは、アリスからボブへのチャネルは、秘密鍵暗号または公開鍵暗号のいずれかが必要である。本論文で提案する方式は、敵対者がプロトコルに参加する相手になりすますことができないように、認証されたチャネルのみを必要とします。(敵対者が転送中のメッセージを修正する試みは、秘密が特別な構造を与えられていれば最後に簡単に検出できるため、ここでは懸念しない)。

b) 受託者グループは動的であることが可能である。すなわち、受託者はスキームを再開する必要なく、グループに参加したり、グループから離脱したりすることができる。モジュール式指数関数法の可換特性により、他者から独立して秘密をロックしたり解除したりすることができる。共有秘密s^l は、参加（離脱）するパーティに送られる必要があり、他のパーティと全く同じ方法でロック（ロック解除）できるようにする。

c) この方式の安全性は、因数分解よりも困難とされるDLPに依存している。その結果、この方式は、例えば、Shamir threshold方式とRSA（アリスとボブの間のプライベートリンク用）を併用した方式よりも安全であることが期待される。

d) 誰が秘密を受け取るかを決めること(すなわち、誰がボブを演じるかを決めること)は、ロックフェーズの後まで遅らせることができる。その場合、受信者は、我々が受託者と呼ぶ人々の中から選ぶことができる。この方式は基本的に変わらない。

5 結論

モジュール指数演算の可換特性を利用して、受託者グループの全会一致のもとに、ある当事者から別の当事者へ安全に秘密を転送する方法を示したものである。提案方式の主な利点は、事前に交換する鍵が不要であることである。この方式は離散対数問題に依存しているため、良好な安全性が期待される。

参考文献

[1] Agrawal, R., Evfimievski, A., and Srikant, R., "Information sharing across private databases," *International Conference on Management of Data (ACM SIGMOD),* ACM Press, 2003.

[2] Clifton, C., Kantarcioglu, M., Vaidya, J., Lin, X., and Zhu, M. Y. "Tools for privacy pre serving distributed data mining," *SIGKDD Explorations* 4, 2, January 2003.

[3] Menezes, A., Oorschot, P., Vanstone, S., *Handbook of Applied Cryptography,* CRC Press, 1997.を参照。

[4] Shamir, A., "How to Share a Secret," *Communications of The ACM,* Vol.22, No.11, November 1979.

[5] Shamir, A., "On Power of Commutivity in Cryptography," *ICALP80,* July 1980.

[6] Weis, Stephen A., *New Foundations for Efficient Authentication, Commutative Crypt-phy, and Private Disjointness Testing,* MIT PhD Dissertation, May 2006.