ハッシュ関数を用いた安全なnチャネルメッセージ伝送

木下研究室　栗山　知也　(工学研究科 電気電子情報工学専攻 201070083)

1 PSMT (Perfectly Secure Message Transmission) と ASMT (Almost Secure Message Transmission)

従来の公開鍵暗号方式では公開鍵の正当性を証明するために認証局のような信頼できる第三者機関が必要であった. それに対して n チャネルメッセージ伝送方式では事前の鍵が不要なため第三者機関も必要ない. そこで本論文では n チャネルメッセージ伝送方式に着目している.
n チャネルメッセージ伝送方式は文書を n 本の通信路を使用して安全に送信する暗号化通信方式である. もし n 本のうちの何本かに文書を盗聴・改竄する敵が潜んでいても, 残りの通信路の情報を用いて文書を復号することができる (図 1).n チャネルメッセージ伝送方式には PSMT と ASMT という方式がある.

図 1: n チャネルメッセージ伝送方式

1.1 PSMT における安全性の定義

n チャネルメッセージ伝送方式において次の 2 つの条件を満たしたものを PSMT と呼ぶ.

1. 敵は送信メッセージに関する情報を何も得られない.(盗聴耐性)
2. 受信者がメッセージを正しく受信できる確率が 100 %である.(改竄耐性)

また, 送信者が受信者に 1 回送信するだけで済む方式を 1-round 方式, 送信者と受信者が相互に r 回やり取りを行う方式を r-round 方式と呼ぶ (図 2).
このとき敵が n 本の通信路のうち t 本に潜んでいるとしたときに PSMT プロトコルが存在するための必要十分条件は, 1-round 方式では $n \geq 3t+1$,2-round 方式では $n \geq 2t+1$ であることが証明されている.

1.2 ASMT における安全性の定義

ASMT における安全性の定義は以下のとおりである.

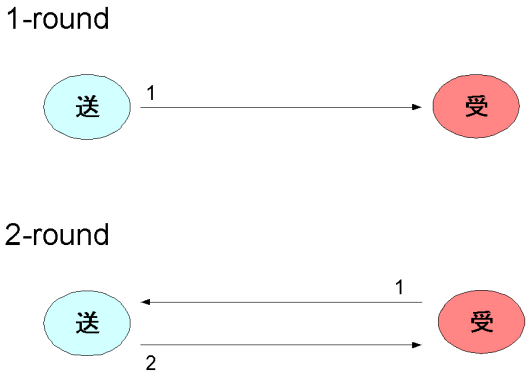

図 2: 1-round 方式と 2-round 方式

1. 敵は送信メッセージに関する情報を何も得られない.(盗聴耐性)
2. 受信者がメッセージを正しく受信できる確率が $1-\delta$ 以上である.(改竄耐性)
3. 受信者が正しく受信できない確率が δ 以下であり, そのとき受信者は failure を出力できる.(失敗検知能力)
4. 敵が t 本の通信路を遮断しても受信者は残りの通信路で得た情報だけからメッセージを受信できる.(遮断耐性)

すなわち上記の安全性が意味するところは送信者が秘密 s を ASMT で送った場合, 受信者は s' あるいは failure を出力する. その時 failure を出力する確率が δ 以下であり,s' を出力した場合は必ず $s'=s$ となることである. PSMT と比較して主に異なる点は定義 2 においてメッセージを正しく受信できる確率が $1-\delta$ となっており, 失敗した時はそれを検知できるという定義 3 が加わっている点である.
Kurosawa らが通信効率を厳密に評価するために以下の定義を提案した.

ASMT プロトコルが次の条件を満たす時, そのプロトコルは Canonical であるという.
(1) n = 2t + 1
(2) ある関数 F が存在し, 次を満たす.

$$\text{送信者の出力} = \begin{cases} s' & if\ F(X'_{i_1},\cdots,X'_{i_{t+1}}) \\ = S'\ or\ \perp & for\ any\ (X'_{i_1},\cdots,X'_{i_{t+1}}) \\ failure & otherwise \end{cases} \tag{1}$$

ただし X'_i は channel(i) を通り受信者が受信した情報とする.
ASMT は 2004 年に Srinathan らによって提案されたが, そのプロトコルには間違いがあった. その後 2007 年に Kurosawa らによって厳密に定義された. そのなかで $n=2t+1$ での通信効率の限界が以下のように示された.
$\mathcal{X}_i$：channel(i) を流れる可能性のある情報の集合
$\mathcal{S}$：送信者が送る可能性のある秘密の集合
δ：失敗確率

A 1-Round Almost Secure Message Transmission Protocol with Hash, Kuriyama TOMOYA(kinoshita laboratory,Graduate School of Electrical, Electronics and Information Engineering).

ASMT プロトコルが Canonical ならば, 次を満たす.

$$|\mathcal{X}_i| \geq (|\mathcal{S}|-1)/\delta + 1 \qquad (2)$$

また,Kurosawa らは通信効率の限界に近い通信量で通信できるプロトコルも提案した. そのプロトコルの通信効率は失敗確率を ϵ とすると,

$$|\mathcal{X}_i| = \frac{|\mathcal{S}|-1}{\delta} + 1 > \frac{|\mathcal{S}|-1}{\epsilon} + 1$$

ただし $\epsilon = \left\{ \begin{pmatrix} n \\ t+1 \end{pmatrix} - \begin{pmatrix} n-t \\ t+1 \end{pmatrix} \right\} \delta$

となっている.

2 Basic プロトコル

2.1 Basic プロトコル

本論文での提案プロトコルの前に基本形である Basic プロトコルを提案する.

Basic プロトコルの特徴はハッシュ関数 H を用いる点である. その手順は $n = 2t+1$(n : 通信路の数,t : 敵の数), 送信する秘密情報を s,P を大きな素数とすると以下のとおりである.

送信者

1. $f(x) = s + a_1 x + a_2 x^2 + \cdots + a_t x^t \mod P$ をランダムに作る.
2. ハッシュ値 $H(f(1)), \cdots, H(f(n))$ を計算する.
3. 各チャンネル ch-i に $f(i), H(f(1)), \cdots, H(f(n))$ を送る.

敵

- $f(1), \cdots, f(n)$ のうち,t 個しか知らない.
  $\rightarrow$ $f(x)$ は t 次関数なので t 点からは s について何も分からない.
- ここでハッシュ関数 H は一方向性があると仮定するので $H(m)$ から m を逆算できない.
  $\rightarrow$ ハッシュ値からは s について何も分からない.

受信者

1. $f'(1), \cdots, f'(n)$ を得る.
2. n 本の通信路のうち半分以上の $t+1$ 本は正しい情報であることを利用し, 多数決を取り正しい $H(f(1))$, $\cdots, H(f(n))$ を得る.
3. $H(f'(1)), \cdots, H(f'(n))$ を計算し, $H(f(1)), \cdots, H\ (f(n))$ と等しいかを調べる.
4. $H(f(i)) = H(f'(i))$ となる $f'(i)$ は $t+1$ 個以上ある. それら全てを通る t 次関数 $f'(x)$ が存在するかどうかはラグランジェの補間公式から容易にわかる. 存在するなら $s' = f'(0)$ を出力し, 存在しなければ failure を出力する.

2.2 Basic プロトコルの計算量

まず送信者について.STEP1 はランダムに関数を作るだけなので, 計算量は多項式時間である. STEP2 は計算量が多項式時間のハッシュ関数を用いるので多項式時間となる.
次に受信者について.STEP2 のハッシュ値同士を比べ, 多数決をとるので計算量は多項式時間である. STEP3 はハッシュ値の計算とハッシュ値同士の比較なので計算量は多項式時間である. そして STEP4 の復号処理はラグランジェの補間公式を用いる. これは多項式時間で計算することができる.
全ての手順は多項式時間で計算することができる. よって全体の計算量も多項式時間である.

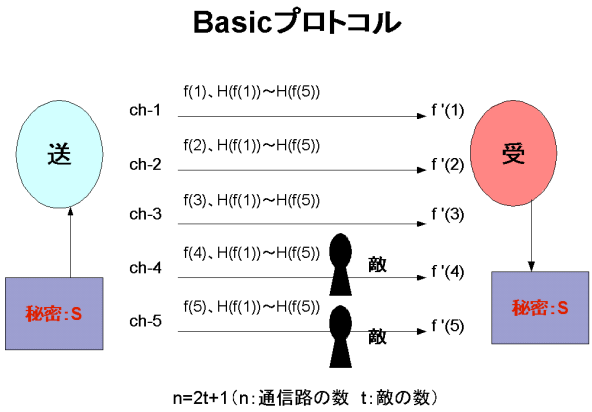

図 3: Basic プロトコル

2.3 Basic プロトコルの通信量

Kurosawa らが提案したプロトコルは計算量が指数関数的であるという問題があった. Basic プロトコルの特徴はハッシュ関数 H を用いて計算量が多項式時間に改善されていることである. 敵の Second Preimage Attack が成功したときがこのプロトコルの失敗となる. 敵は t 個のハッシュ値に Second Preimage Attack をするので, このプロトコルの失敗確率 ϵ は,

$$\epsilon \leq [\text{ハッシュ関数 } H \text{ への } SecondPreimageAttack \text{ が成功する確率}] \times t \qquad (3)$$

ここで H の出力値のビット数を h とすると, 出力値は 2^h 通りとなり, H がランダムオラクル (ランダムに値を出力する) と仮定すると H への Second Preimage Attack が成功する確率は $1/2^h$ となる. ハッシュ値への衝突攻撃の試行回数を k とする. したがって式 (3) は

$$\epsilon \leq (\frac{t}{2^h})k \qquad (4)$$

となる.

3 提案プロトコル

提案プロトコルでは Basic プロトコルと違い,1 度に m 個の s_i を送ることで通信効率を改善している. 提案プロトコルの手順は以下のとおりである.
但し,H はハッシュ値であり, 安全なハッシュ関数を用いるとする.
$n = 2t+1$(n : 通信路の数,t : 敵の数), 送信する秘密情報を $s = \{s_1, \cdots, s_m\}$,P を大きな素数とする.

送信者

1. $f_1(x), \cdots, f_m(x)$ をランダムで決める.($f_i(x) = s_i + a_{i_1} x + a_{i_2} x^2 + \cdots + a_{i_t} x^t$)
2. $\boldsymbol{F}_1 = f_1(1) \| f_2(1) \| f_3(1) \| \cdots \| f_m(1)$
   $\boldsymbol{F}_2 = f_1(2) \| f_2(2) \| f_3(2) \| \cdots \| f_m(2)$
   $\vdots$
   $\boldsymbol{F}_n = f_1(n) \| f_2(n) \| f_3(n) \| \cdots \| f_m(n)$ とおく.
3. ハッシュ値 $H(\boldsymbol{F}_1), \cdots, H(\boldsymbol{F}_n)$ を計算する.
4. 各チャンネル ch-i に $\boldsymbol{F}_i$,$H(\boldsymbol{F}_1), \cdots, H(\boldsymbol{F}_n)$ を送る.

敵

- $\boldsymbol{F}_1, \cdots, \boldsymbol{F}_n$ のうち,t 個しか知らない.
  $\rightarrow$ $\boldsymbol{F}_i$ 中の $f_i(x)$ は t 次関数なので t 点からは s について何も分からない.

- ここでハッシュ関数 H は一方向性があると仮定するので $H(m)$ から m を逆算できない.
  → ハッシュ値からは s について何も分からない.

受信者

1. $\boldsymbol{F}'_1, \cdots, \boldsymbol{F}'_n$ を得る.
2. n 本の通信路のうち半分以上の $t+1$ 本は正しい情報であることを利用し, 多数決で正しい $H(\boldsymbol{F}_1), \cdots, H(\boldsymbol{F}_n)$ を得る.
3. $H(\boldsymbol{F}'_1), \cdots, H(\boldsymbol{F}'_n)$ を計算し, $H(\boldsymbol{F}_1), \cdots, H(\boldsymbol{F}_n)$ と等しいか調べる.
4. $H(\boldsymbol{F}_i) = H(\boldsymbol{F}'_i)$ となる $\boldsymbol{F}'_i$ は $t+1$ 個以上ある. それら全てを通る t 次関数 $f'_i(x)$ が存在するかどうかはラグランジェの補間公式から容易にわかる. 存在するなら $s' = \{f'_1(0), \cdots, f'_m(0)\}$ を出力し, 存在しなければ failure を出力する.

3.1 提案プロトコルの計算量

提案プロトコルでは 1 度に m 個の秘密を送るので,Basic プロトコルの約 m 倍の計算量が必要である. しかし,$m = O(n)$ であれば多項式時間のものを m 倍しても多項式時間であるので, 提案プロトコルの計算量は多項式時間である.

3.2 提案プロトコルの通信量

提案プロトコルは 1 度に m 個の秘密を送ることにより, その分のハッシュ値の通信量が削減され通信効率が良くなっている. Basic プロトコルを用いて m 個秘密を送る場合と比較し, 評価する. まず Basic プロトコルの通信量を計算する. 秘密 s の長さを q ビット,m 個の秘密 s を送るとき, 送信者が送る可能性のある秘密の集合 $\mathcal{S}$ と channel(i) を流れる可能性のある情報の集合は $\mathcal{X}_{1_i}$ は

$$|\mathcal{S}| = (2^q)^m, |\mathcal{X}_{1_i}| = (2^{q+hn})^m \tag{5}$$

次に提案プロトコルの計算量を計算する. 秘密 s の長さを q ビット,m 個の秘密 s を送るとき, 送信者が送る可能性のある秘密の集合 $\mathcal{S}$ と channel(i) を流れる可能性のある情報の集合は $\mathcal{X}_{2_i}$ は

$$|\mathcal{S}| = 2^{qm}, |\mathcal{X}_{2_i}| = 2^{qm+hn} \tag{6}$$

送信者が送る可能性のある秘密の集合 $\mathcal{S}$ を channel(i) を流れる可能性のある情報の集合 $\mathcal{X}_i$ で割ったものを通信レートとする.

通信レート $= \frac{|\mathcal{S}|}{|\mathcal{X}_i|}$

式 (5), 式 (6) より Basic プロトコルと提案プロトコルの通信レートを計算し, 比較すると

$$\frac{\frac{|\mathcal{S}|}{|\mathcal{X}_{1_i}|}}{\frac{|\mathcal{S}|}{|\mathcal{X}_{2_i}|}} = \frac{\frac{2^{qm}}{2^{qm+hn}}}{\frac{2^{qm}}{2^{qm+hn}}} = \frac{2^{-hn}}{(2^{-hn})^m} = 2^{hn(m-1)} \tag{7}$$

となる. 以上より提案プロトコルは Basic プロトコルより通信効率が改善されていることがわかる.

提案プロトコルの失敗確率 ϵ を求め,Basic プロトコルを用いて m 個秘密を送る場合と比較して評価する. Basic プロトコルでの失敗確率 ϵ は式 (4) より

$$\epsilon \leq (\frac{t}{2^h})k$$

m 個秘密を送る場合は敵は mt 個のハッシュ値に Second Preimage Attack をするので

$$\epsilon \leq (\frac{mt}{2^h})k \tag{8}$$

となる. 提案プロトコルの失敗確率 ϵ は t 個のハッシュ値に Second Preimage Attack をするので

$$\epsilon \leq (\frac{t}{2^h})k \tag{9}$$

$$(\frac{t}{2^h})k \leq \epsilon \leq (\frac{mt}{2^h})k \tag{10}$$

となる. 以上より提案プロトコルは Basic プロトコルより失敗確率が改善されていることがわかる.

秘密 s の長さを q ビットとおくと, 送信者が送る可能性のある秘密の集合 $\mathcal{S}$ と channel(i) を流れる可能性のある情報の集合は $\mathcal{X}_i$ は

$$|\mathcal{S}| = 2^{qm}, |X_i| = 2^{qm+hn} \tag{11}$$

となる.

提案プロトコルは Canonical であるから通信効率の限界を計算すると

$$\delta \geq \frac{2^{qm}-1}{2^{qm+hn}-1} \approx \frac{1}{2^{hn}} \tag{12}$$

式 (9) と式 (12) より

$$\frac{1}{2^{hn}} \leq \delta \leq \frac{kt}{2^h} \tag{13}$$

ここでは k と t が十分小さいとしても通信効率の限界と比べると $\frac{1}{2^n}$ だけ差があることがわかる. 計算量が多項式時間のままこの差を埋めることが今後の課題である.

4 提案プロトコルの実装

ｎチャネルメッセージ伝送の実装にはいくつかの問題点がある.

1. 最短経路だけでない経路の確保
2. 経路の探索とその最適

1 つ目の問題について. ｎチャネルメッセージ伝送とはｎ本の通信路によって暗号化通信する方式である. ここでいうｎ本の通信路というのは異なる通信経路がｎ本必要だということになる. しかしながら現在のインターネットでは経路制御表に従い最も最短経路を通るという大原則がある. そのため, 何かしらの工夫を施し最短経路だけでない異なるｎ本の通信路を確保する必要がある.
2 つ目の問題について. 上では異なるｎ本の経路をとる必要があるという問題点をあげた. しかし問題はそれだけではなく、何らかの工夫を施して最短経路以外を通り、ｎ本の経路を通ることが可能になったとしても毎回同じ経路を通り, 毎回同じ相手とやりとりをするわけではないので経路自体を自分で選び出せる必要がある. また, 経路上に潜む敵が多くては通信が困難になる恐れがある. その他にもあまりにも近い経路を通るのでは分岐した部分でしか安全性を確保できない. そのような観点から敵の存在を考慮した経路の選択が必要となってくることがわかる.

4.1 意図した経路の確保

複数の異なる経路をとる方法としてはインターネット上に経由専用のサーバを複数立てるなどいくつかの方法が考えられるが、認証局がいらないという利点を活かす意味でも送信者と受信者だけで通信できる方法を模索した．そこでソースルーティングを採用した．ソースルーティングとは送信者が明示的に経路を指定することができるようになる方式である．最短経路ではない地点を指定することで異なる複数経路をとることができる．

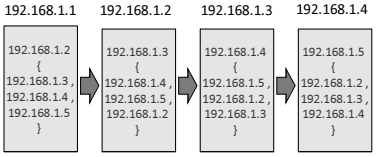

図 4: ソースルーティングによる IP ヘッダの動き

4.2 最適経路の選択

意図した経路をとることができるようになり、異なるｎ本の経路をとることが可能となった．しかし、指定した地点へ分岐する前や後の地点に敵が潜んでいては複数経路では安全性が損なわれてしまう．現在のインターネットでは送信者はプロバイダを通して受信者と通信している．プロバイダが同じあれば同じプロバイダ内で、違うプロバイダであればプロバイダ間での経路が発生する．送信者と受信者のプロバイダ内のルータは経由させても数が少なく最後には必ず自分に１番近いルータをとるため効果が薄いと考えられる．よって、１番に考えなければならないのがが送信者と受信者が違うプロバイダを使っている場合の経路についてとなる．

4.3 実装と実験手順

Oracle 社の VM VirtualBox を使い仮想環境で実験を行った．（図 5）オペレーテイングシステムには Ubuntu10.10 を使用した．また、ソースルーティングはデフォルトでは禁止にされているので sysctl の設定を変更する．$net.ipv4.conf.all.accept\_source\_route = 1$

実験手順

1. それぞれのホストの出口と入口で tcpdump を行いパケットを監視する．
2. 受信者が受信プログラムを実行する．
3. 送信者が送信プログラムを実行する．
4. 受信者の受信プログラムが正しく情報を受信し、復号できていることを確認する．
5. tcpdump を行った箇所で正しくソースルーティングが行われたかを確認する．

ここでは受信プログラムは各チャネルから受け取った情報を元に復号し、その結果を表示する．また、送信プログラムは入力された秘密を暗号化し、ストリクトソースルーティングを用いて各チャネルを通り受信者に暗号化された情報を送る．

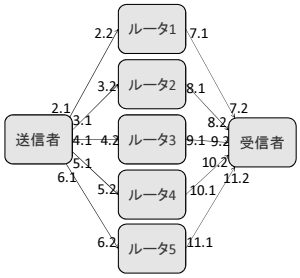

図 5: 実験装置の配置

4.4 実験結果

受信プログラムの結果より正しく秘密が復号されていることを確認した．また、各アドレスの tcpdump の結果からもソースルーティングが正しく行われ、暗号化された情報が受信者に届いたことが確認された．

5 まとめ

ハッシュ関数を用いた ASMT プロトコルを提案した．ASMT は 2007 年に Kurosawa らによって厳密に定義された．そのなかで $n = 2t + 1$ のときの通信効率の限界が示され，限界に近い通信量で通信できるプロトコルが提案された．しかしそこのプロトコルは計算量が指数関数的であるという問題があった．提案プロトコルはハッシュ関数を用いることでこれを多項式時間まで改善した．提案プロトコルの通信効率は通信効率の限界と比べると $\frac{1}{2^n}$ だけ差があることがわかった．ｎチャネルメッセージ伝送はまだ実装がなされていない暗号化通信方式である．これをソースルーティングを用いて提案したプロトコルを実装した．

参考文献

[1] DANNY DOLEV,CYNTHIA DWORK,ORLI WAARTS,MOTI YUNG ”Perfectly Secure Message Transmission”
Journal of the Association for Computing Machinery,Vol.40,No.1,
pp.17-47(1993)

[2] K. Srinathan,Arvind Narayanan,C. Pandu Rangan ”Optimal Perfectly Secure Message Transmission”
CRYPTO 2004,LNCS 3152,pp.545-561(2004)

[3] Kaoru KUROSAWA,Kazuhiro SUZUKI,Members ”Almost Secure (1-Round,n-Channel) Message Transmission Scheme”
IEICE TRANS. FUNDAMENTALS,VOL.E92-A,NO.1(2009)

[4] HASAN MD. SAYEED,HOSAME ABU-AMARA ”Efficient Perfectly Secure Message Transmission in Synchronous Networks”
INFORMATION AND COMPUTATION 126,pp.53-61(1996),ARTICLE NO.0033

[5] Saurabh Agarwal,Ronald Cramer,Robbert de Haan ”Asymptotically Optimal Two-Round Perfectly Secure Message Transmission”
CRYPTO 2006,LNCS 4117,pp.394-408(2006)

[6] Kaoru Kurosawa,Kazuhiro Suzuki ”Truly Efficient 2-Round Perfectly Secure Message Transmission Scheme”
Advances in Cryptology,EUROCRYPT 2008 LNCS 4965,pp.324-340(2008)