ビット委託方式の効率化の研究
Improvements on the Efficiency for Bit Commitment Schemes

プロジェクト代表者：小柴健史（理工学研究科・准教授）
英語表記　Takeshi　Koshiba

１　はじめに

コンピュータネットワークの安全性を守る情報セキュリティ技術の一つに暗号技術があるが、暗号技術はデータの安全性を守る「秘匿技術」と対象（人やデータ）の真正性を保証する「認証技術」に大別される。究極の認証技術として、対象の性質は一切漏らさずに真正性を相手に納得させる手法（ゼロ知識認証）がある。さらに、ゼロ知識認証の基礎技術にビット委託方式と呼ばれる技術があり、例えば「相手が不正直」でも公平に「電話でじゃんけん」をすることを可能にする通信プロトコルである。

ビット委託方式には「受信者が不正直な場合」と「送信者が不正直な場合」の２通りのどちらを主に考えるかによって２種類の方式が存在する。特に後者の、送信者が不正直な場合についてのビット委託方式は効率的な方法が知られておらず、通信手順数が非常に多い方法が知られているのみである。一方、前者の送信者が不正直な場合では、通信手順数が定数回となる方法が知られており、ビット委託方式の既存技術は通信手順数という観点から見た場合、アンバランスな状況にある。そこで、送信者が不正直な場合でも、通信手順数が少なくても済むような方式が強く望まれている。これが実現されれば、ビット委託方式をビルディングブロックとする各種セキュアプロトコルの設計の自由度を高めることが可能となる。なぜならば、ビット委託方式はセキュアプロトコルの中では「ネジ・クギ」に相当する基本部品だからである。

２　従来技術、研究成果およびその評価

［ビット委託方式］

ビット委託方式は2者間の2フェーズプロトコルで、委託フェーズと開示フェーズで構成されている。送信者Sは秘密のビット情報bをそのビット情報を漏らさずに受信者Rに暗号化された状態で転送する。委託フェーズで受信者Rがビット情報bを知ることができないという性質を秘匿性と呼ぶ。開示フェーズでは送信者Sはビット情報bが何であったかを受信者Rに伝える。このとき、送信者Sは偽の開示情報を送信することも可能であるが、受信者Rは偽の開示情報と委託されているビット情報bの暗号化情報から送信者Sが騙そうとしていることを見破ることができることが望ましく、この性質を束縛性と呼ぶ。

［従来技術］

ビット委託プロトコルの一つとして完全束縛性をもつ従来方式としてNaor-Ostrovsky-Venkatesan-Yung(NOVY方式)による一方向性置換に基づく方式が知られているが、まず、NOVY方式について紹介する。

委託フェーズ：

1. 送信者Sはnビットのビット列xを一様ランダムに選択し、y=f(x)を計算。ただし、fは一方向性置換。bを委託ビットとする。
2. k=1,…,n-1について以下を行う。(以下で、ビット列はGF(2)上のn次元ベクトルと見なし、<>は内積を表す)
   (ア) 受信者Rは$h_k \in 0^{k-1}1\{0,1\}^{n-k}$から一様ランダムに選択し、送信者Sに送る。
   (イ) 送信者Sは$c_k=<y,h_k>$を受信者Rに送る。

3. 送信者Sは連立方程式$c_1=<z,h_1>,\ldots,c_{n-1}=<z,h_{n-1}>$を求解し、その解を辞書式順序で$z_0,z_1$とする。yと一致する方を$z_d$とし$e=b+d(\mathrm{mod}2)$を受信者Rに送る。
4. 受信者Rの方でも同様に連立方程式をとき、z_0,z_1を求めておく。

開示フェーズ：

5. 送信者Ｓはbとxを受信者Rに送る。
6. 受信者Rは$y'=f(x)$を計算し、各$c_i=<h_i,y'>$が成立していることを確認する。$d=b+e(\mathrm{mod}2)$を計算し、$y=y_d$のときに送信者Sは偽の開示を行っていないと判断し、ビット情報bを受け入れる。

NOVY方式は委託フェーズn-1ラウンドの通信回数になっていることが分かる。このNOVY方式の計算量理論的束縛性はhが対独立ハッシュ関数族を構成している事実と各ラウンドの通信内容の相関が小さいためChebyshevの不等式を巧みに利用した確率評価技法を用いて、送信者Sが偽の開示で受信者Rを騙すアルゴリズムから一方向性置換fの逆関数計算への帰着を与えることによって数学的に証明されている。一方、完全秘匿性については情報理論的な議論を用いて比較的容易に証明される。

［研究成果］

委託フェーズの２(ア)の情報を$O(\log n)$個まとめて送信し、ラウンド数を$O(n/\log n)$とすることに成功した。まとめ送信により各ラウンドの相関が非常に高くなり、まとめて送るh_iはもはや対独立という性質を失ってしまうため、従来技法の評価ができないのだが、まとめて送るh_iに関しての平均的性質を究明し、それを評価するための確率的技法を新規に開発することにより、NOVY方式の計算量理論的束縛性の証明を数学的に与えることができるようになった。

［評価］

NOVY方式で用いている技法はInteractive Hashing技法と呼ばれるが、その後、HaitnerとRaingoldによりInteractive Hashing技法の性質の研究がなされ、今回の研究成果とは独立に論文[2]の発表直後に$O(n/\log n)$が達成できることが証明された。さらに、2007年2月にWeeによって特殊条件下では$\Omega(n/\log n)$より改善出来ないことが証明され、2007年4月にHaitner, Hoch, Reingold, Segevによって一般に$\Omega(n/\log n)$より改善出来ないことが証明された。このため、今回の研究成果での改善が一般の完全秘匿ビット委託方式のラウンド数に関しての最善方式であることが保証されたことになる。

３　発表論文

[1] Takeshi Koshiba, Yoshiharu Seri, "Reducing the Round Complexity of NOVY Interactive Hashing by Logarithmic Factor," 2007 年暗号と情報セキュリティシンポジウム, SCIS 2007 (佐世保, 2007.1.24), 2A3-3.

[2] Takeshi Koshiba, Yoshiharu Seri, "Round-Efficient One-Way Permutation Based Perfectly Concealing Bit Commitment Scheme," Electronic Colloquium on Computational Complexity, TR06-093, 2006.