SCIS 2006 The 2006 Symposium on Cryptography and Information Security
Hiroshima, Japan, Jan. 17-20, 2006
The Institute of Electronics, Information and Communication Engineers

リアルタイム無証拠 Schnorr 認証
Realtime Receipt Free Schnorr Identification

星野 文学* 小林 鉄太郎 * 鈴木 幸太郎 *
Fumitaka Hoshino Tetsutaro Kobayashi Koutarou Suzuki

あらまし 本研究では 認証プロトコルに於いて honest な検証者と観察者を仮定しても通信記録が認証成功の証拠とならない性質 “リアルタイム無証拠性” の概念を提案する. さらに Schnorr 認証 [Sch91] において リアルタイム無証拠性と 他の安全性要件である健全性が一見両立困難 なように思えるが, 使用する巡回群に構造を持ったモデルを導入するとプロトコルを変更せずに両立できる事を示す. そして 特殊な楕円曲線で生成した群の系列 [SHUK03, SHUK04] を用い, 使用する群の選択がプロトコルの安全性にどのような影響をあたえるか検討し, 構造を持った群でプロトコルを構成する場合, 群の安全性は DDH 安全だけでは不十分である事を示す.

キーワード Realtime Receipt Free, Schnorr Identification, Elliptic Curve

1 はじめに

G を DDH 安全な素数位数の巡回群 (位数 ℓ) として $g, y \in_U G$ が公開されているとする. $y = g^x$ なる $x \in \mathbb{Z}_\ell^+$ を知る証明者が, x に関する知識を所有する事を効率的に対話証明する方法はよく知られている.[Sch91, Oka93]

[**Schnorr 認証**]

Step.1 **証明者 → 検証者**
証明者は乱数 $r \in_U \mathbb{Z}_\ell^+$ を用い $R = g^r$ を求め R を検証者へ送る.

Step.2 **証明者 ← 検証者**
検証者はチャレンジ $c \in_U \mathbb{Z}_\ell^+$ を証明者に送る.

Step.3 **証明者 → 検証者**
証明者は $z = r - cx$ を求め z を検証者へ送る. 検証者は $R = g^z y^c$ ならば証明者が x に関する知識を所有する事を納得する.

さらに Fiat-Shamir heuristic[FS86] を用いる事によって非対話証明を構成することも可能である. こうしたテクニックは 1980 年代後半頃から盛んに研究され非常に多くの暗号プロトコルに用いられてきた.

この Schnorr 認証のプロトコルにおいて, 認証に用いられたメッセージの単純な記録は認証が成功した事に対する証拠とはならない. しかしながら, honest な検証者を仮定すると, プロトコルをリアルタイムで観察している任意の第三者が検証者と同じ方法を用いて認証が失敗したのか成功したのか判定する事が出来る. この事は honest な検証者と, 通信をリアルタイムで記録する honest な観察者を仮定すると, 通信記録が認証成功の証拠として機能する事に他ならない.

認証プロトコルがこうした性質を持つと, 例えば計算機に外部からログインしたとき, やり取りしたメッセージに知らぬ間にタイムスタンプが押され, 後に ログインの証拠として, 無関係の人間に勝手に利用されてしまうかもしれない. あるいは非接触のスマートカードが発する電磁波を何者かが勝手に記録し, せっかくの完璧なアリバイを崩す決定的な証拠となってしまうかもしれない.

honest な検証者と観察者を仮定しても通信記録が認証成功の証拠とならない性質を, リアルタイム無証拠性と呼ぶ事にする. Schnorr 認証で Step.2 と Step.3 のメッセージを g の冪に載せて送ると G の DDH 安全性に基づき, 計算量的にリアルタイム無証拠性を担保する事が出来る. 即ち

[G-**Schnorr 認証**]

Step.1 **証明者 → 検証者**
証明者は乱数 $R \in_U G$ を検証者へ送る.

Step.2 **証明者 ← 検証者**
検証者は乱数 $c \in_U \mathbb{Z}_\ell^+$ を用い $C = g^c$ を求め C を証明者に送る.

Step.3 **証明者 → 検証者**
証明者は $Z = RC^{-x}$ を求め Z を検証者へ送る. 検証者は $R = Zy^c$ ならば証明者が x に関する知識を所有する事を納得する.

* NTT 情報流通プラットフォーム研究所, 神奈川県横須賀市光の丘 1-1,NTT Information Sharing Platform Laboratories,1-1 Hikarinooka Yokosuka-Shi Kanagawa 239-0847 Japan

だがこのプロトコルは健全性を証明出来ない. 健全性とは 秘密鍵 x に関する非自明な情報を知らない限り偶然より高い確率では証明者へのなりすまし が成功しない性質の事である. 高い確率で なりすましが成功する R を知っているなら多項式時間で x に関する非自明な情報を取り出せる事が示せれば証明出来る.

上記の場合, 異なる (C_0, Z_0), (C_1, Z_1) が同じ R に対する認証となるとき, $C_0C_1^{-1}$ 及び $Z_0^{-1}Z_1$ に関する離散対数が x の非自明な情報となるが, 群 G が離散対数困難であった為に健全性が証明できない. 従ってこの方法は必ずしも健全とは限らない.

Schnorr 認証の場合は この部分が $\mathbb{Z}_\ell^+$ の元であったので $c_0 - c_1$ 及び $z_1 - z_0$ から簡単に x を求める事ができて, 健全性が証明できる.

1980 年代後半に こうした研究が行われていた頃, 安全で実用的な巡回群 G として想定されていたのは $\mathbb{Z}_p^*$ の部分群であった. 現在では 楕円曲線暗号等の発達により G として利用可能な巡回群が幾分豊富になっている.

ところで $\mathbb{Z}_\ell^+$ の代わりに使用可能な群は豊富に存在するだろうか ? 楕円曲線を使うと $\mathbb{Z}_\ell^+$ の代わりとなる群を比較的簡単に得ることが出来る. 本研究では, Schnorr 認証において暗号学的安全性が $\mathbb{Z}_\ell^+$ より強く上記の G よりは弱い幾つかの現実的な群を, $\mathbb{Z}_\ell^+$ の代わりに使用することによってプロトコルの安全性にどのような変化が生じるか検討しその安全性を議論する.

2 準備

pairing が計算可能な楕円曲線を使うと DDH は解けるが CDH は困難と思える巡回群を構成できる事がよく知られている. また, 著者らは DDH 安全な群と CDH 安全な群の中間的な性質をもつ群, Revocable DDH Group を提案し, ある楕円曲線の設定 [SHUK03, SHUK04] を用いて実現方法を示した [HSK05].

本研究では, 楕円曲線に関する一方向同型写像で結ばれた群の系列を用いて, Schnorr 認証の安全性を議論する. ここで, この系列に関する事実を簡単にまとめておく.

2.1 A Special Bilinear Group

非 trace-2 非超特異楕円曲線を使うと以下のような一方向同型写像で結ばれた群の系列を得ることが出来る [SHUK03, SHUK04].

$$\mathbb{Z}_\ell^+ \to \mathbb{G}_1 \to \mathbb{G}_2 \to \mathbb{G}_3$$

$\mathbb{G}_1$ と $\mathbb{G}_2$ はそれぞれ楕円曲線の位数 ℓ の 部分群でである. $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3$ の間には pairing と呼ばれる双線形写像

$$\mathrm{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_3$$

が定義されている. e の入力において, $\mathbb{G}_1$ の元を固定すれば, $\mathbb{G}_2 \to \mathbb{G}_3$ の同型写像を得ることが出来る. この同型写像は pairing を暗号プリミティブとして使うような場合には一方向であると信じられている. また, $\mathbb{G}_1, \mathbb{G}_2$ の間には

$$\psi : \mathbb{G}_1 \to \mathbb{G}_2$$

なる同型写像があるとする. 非 trace-2 の 非超特異楕円曲線で $\mathbb{G}_1$ がフロベニウス写像の非固有空間, $\mathbb{G}_2$ が固有空間 である場合に一方向と思われる ψ の候補が提案されている [SHUK03, SHUK04].

2.2 Decisional co-Diffie-Hellman 問題

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3$ の群の系列の中で $\mathbb{G}_1$ だけが DDH 安全ではない. 即ち $\mathcal{G}, \mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3 \in \mathbb{G}_1$ を DDH 問題のインスタンスとすると

$$\mathrm{e}(\mathcal{G}, \psi(\mathcal{G}_3)) \stackrel{?}{=} \mathrm{e}(\mathcal{G}_1, \psi(\mathcal{G}_2))$$

により多項式時間で解を得ることが出来る. 一方 $\mathbb{G}_2, \mathbb{G}_3$ 上での DDH 問題を多項式時間で解く方法は知られていない.

では $\mathbb{G}_2, \mathbb{G}_3$ が両方とも DDH 安全だと仮定して, 両者は暗号学的に等価な存在であるといえるだろうか ? 本節で $\mathbb{G}_2$ と $\mathbb{G}_3$ の暗号学的安全性の違いを定義し, 後の章で この違いがプロトコルの安全性に大きな違いをもたらす事を示す. 自明な事ではあるが, この事は 構造を持った群を活用してプロトコルを構成する場合に群に求められる安全性が単なる DDH 安全では済まない事を意味している.

[定義] Decisional co-Diffie-Hellman 問題

G_1, G_2 を同じ位数の巡回群とし, $g \in G_1$, $\mathcal{G} \in G_2$ をそれぞれ生成元とする. (G_1, G_2) 上の Decision co-Diffie-Hellman 問題とは与えられた $(g, g^a, \mathcal{G}^b, \mathcal{G}^c)$ の組から $c = ab$ であるか否かを決定する事である. 以後 co-DDH 問題と記す. また 群 G_1 上の G_2-co-DDH 問題とは (G_1, G_2) 上の co-DDH 問題の事である.

[Proposition]

G_2 から G_1 への多項式時間同型写像が存在するとき (G_1, G_2) 上の co-DDH 問題は G_2 上の DDH 問題より難しく G_1 上の DDH 問題より易しい.

表 1 は, 上記の一方向同型写像で結ばれた $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3$ がもつ暗号学的な性質の違いを示す. 一方向の下流へ行くほど暗号を構成するのに適した “安全な群” になる. 下流の群で DLP/DDH/co-DDH が破れると上流の群の同じ問題も解ける. 下流の群で CDH が破れた場合, 必ずしも上流へは伝播しないが, 上流の群の DDH はすべて破れる.

[Assumption.1] $\mathbb{G}_3$ 上の $\mathbb{G}_1$-co-DDH 問題は難しい.

表 1: 問題の難しさ

	DL(CDH)	DDH	$\mathbb{G}_1$-co-DDH
$\mathbb{Z}_q^+$	easy	easy	easy
↓			
$\mathbb{G}_1$	?	easy	easy
↓			
$\mathbb{G}_2$	?	?	easy
↓			
$\mathbb{G}_3$	?	?	?

[**Assumption.2**] $\mathbb{G}_3$ 上の $\mathbb{G}_2$-co-DDH 問題は難しい.
[**Fact.1**] $\mathbb{G}_2$ 上の $\mathbb{G}_1$-co-DDH 問題は易しい.

後で健全性を証明するのに便利な以下の定義と仮定を与えておく. これらは, $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3$ 間の同型写像が一方向であるとする仮定を幾分強めたものとなっている.

[**定義**] **Pairwise co-Diffie-Hellman 問題**

G_1, G_2 を同じ位数の巡回群とし, $g \in G_1$, $\mathcal{G} \in G_2$ をそれぞれ生成元とする. (G_1, G_2) 上の Computational Pairwise co-Diffie-Hellman 問題とは $y \in G_1$ が与えられたとき,

$$\text{co-DDH}(g, y, \mathcal{G}_0, \mathcal{G}_1) = \text{true}$$

を満たす $\mathcal{G}_0, \mathcal{G}_1 \in G_2$ を求める事である. 以後 co-pDH 問題と記す. また 群 G_1 上の G_2-co-pDH 問題とは (G_1, G_2) 上の co-pDH 問題の事である.

[**Proposition**]

G_2 から G_1 への同型写像 ψ が $g = \psi(\mathcal{G})$ を満たし, $(\mathcal{G}_0, \mathcal{G}_1) = \text{co-pDH}(g, y)$ の時, $\mathcal{G}_0 = \mathcal{G}$ であるなら, $\mathcal{G}_1 = \psi^{-1}(y)$ である.

[**Proposition**]

G_1 から G_2 への多項式時間同型写像が存在し既知であるなら (G_1, G_2)-co-pDH 問題は易しい.

[**Assumption.3**] $\mathbb{G}_3$ 上の $\mathbb{G}_1$-co-pDH 問題は難しい.
[**Assumption.4**] $\mathbb{G}_3$ 上の $\mathbb{G}_2$-co-pDH 問題は難しい.
[**Assumption.5**] $\mathbb{G}_2$ 上の $\mathbb{G}_1$-co-pDH 問題は難しい.
[**Fact.2**]

$\mathbb{G}_2$ 上の $\mathbb{G}_1$-co-pDH 問題が易しいなら $\mathbb{G}_2$ 上の DDH 問題は易しい.

3 (G_1, G_2)-Schnorr 認証

最初に紹介した Schnorr 認証では, 第一メッセージは DDH 安全な G 上の元, 第二第三メッセージは $\mathbb{Z}_\ell^+$ 上の元であった. 後の便宜を図るために (G_1, G_2)-Schnorr 認証を第一メッセージおよび公開鍵が G_1 上の元, 第二第三メッセージが G_2 上の元であるような Schnorr 認証であるとする. この定義に従えば通常の Schnorr 認証は $(G, \mathbb{Z}_\ell^+)$-Schnorr 認証, G-Schnorr 認証は (G, G)-Schnorr 認証ということになる. 後に G_1, G_2 に $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_3$ を代入して安全性の検討を行う.

[**定義**] (G_1, G_2)**-Schnorr 認証**

公開パラメタ

G_1 の生成元 g, G_2 の生成元 $\mathcal{G}$, 及び

$$1 \to \mathcal{G} \xrightarrow{\psi} g$$

を満たす一方向準同型写像 ψ.

秘密鍵 $x \in_U \mathbb{Z}_\ell^+$

公開鍵 $y = g^x$

Step.1 証明者 → 検証者

証明者は乱数 $r \in_U \mathbb{Z}_\ell^+$ を用い $R = g^r$ を求め R を検証者へ送る.

Step.2 証明者 ← 検証者

検証者は乱数 $c \in_U \mathbb{Z}_\ell^+$ を用い $\mathcal{C} = \mathcal{G}^c$ を求め $\mathcal{C}$ を証明者に送る.

Step.3 証明者 → 検証者

証明者は $\mathcal{Z} = \mathcal{G}^r \mathcal{C}^{-x}$ を求め $\mathcal{Z}$ を検証者へ送る. 検証者は $R = \psi(\mathcal{Z}) y^c$ ならば 証明者が x に関する知識を所有する事を納得する.

[**健全性**]

同じ R に対する異なる $(\mathcal{C}_0, \mathcal{Z}_0), (\mathcal{C}_1, \mathcal{Z}_1)$ の組から x に関する自明でない情報が求められる.

[**定理**]

同じ R に対する異なる $(\mathcal{C}_0, \mathcal{Z}_0), (\mathcal{C}_1, \mathcal{Z}_1)$ の組から

$$\text{co-DDH}(g, y, \mathcal{G}_0, \mathcal{G}_1) = \text{true}$$

となる情報 $(\mathcal{G}_0, \mathcal{G}_1)$ を guess する事が出来る.

[**証明**]

$$\begin{aligned} \mathcal{G}_0 &= \mathcal{C}_0 \mathcal{C}_1^{-1} \\ \mathcal{G}_1 &= \mathcal{Z}_0^{-1} \mathcal{Z}_1 \end{aligned}$$

[**リアルタイム無証拠性**]

$(g, y, R, \mathcal{C}, \mathcal{Z})$ の組が $(g, g^x, g^r, \mathcal{G}^c, \mathcal{G}^{r-cx})$ の関係を満たすか否か判定できない.

[**定理**]

(G_1, G_2)-co-DDH 問題が安全なら (G_1, G_2)-Schnorr 認証はリアルタイム無証拠性を担保する.

[**証明**]

(G_1, G_2)-Schnorr 認証のリアルタイム無証拠性を破る多項式時間アルゴリズム $\mathcal{A}$ が存在するとき, (G_1, G_2)-co-DDH 問題は以下の多項式時間アルゴリズムに帰着する.

Step.1

co-DDH 問題のインスタンス $(g, y, \mathcal{G}_0, \mathcal{G}_1)$ が与えられる.

Step.2

乱数 $r \in_U \mathbb{Z}_\ell^+$ を用い $R = g^r$, $\mathcal{Z} = \mathcal{G}^r/\mathcal{G}_1$ を計算する.

Step.3

リアルタイム無証拠性攻撃オラクル $\mathcal{A}$ に対し

$$b = \mathcal{A}(g, y, R, \mathcal{G}_0, \mathcal{Z})$$

により, 判定結果 b を得る.

Step.4

co-DDH$(g, y, \mathcal{G}_0, \mathcal{G}_1) = b$ を出力.

プロトコルに健全性およびリアルタイム無証拠性があるか否かは G_1, G_2 に代入する群の性質に依存する. 但し通常の Schnorr 認証のように 健全性を持つためには G_1 は G_2 より "安全な群" を用いる必要がある. また, G-Schnorr 認証のようにリアルタイム無証拠性を持つためには 少なくとも G_1 は DDH 安全である必要がある. $\mathbb{G}_1$ は DDH 安全でないので G_1 として用いる事は出来ない. 一方 G_2 に $\mathbb{G}_1$ を用いる事は問題ない. これらの事を考慮すると (G_1, G_2) として $(\mathbb{G}_3, \mathbb{G}_1)$, $(\mathbb{G}_3, \mathbb{G}_2)$, $(\mathbb{G}_2, \mathbb{G}_1)$ のいずれかを考える事に意味があると思われる.

[**Proposition**]

$(\mathbb{G}_3, \mathbb{G}_1)$-Schnorr 認証において Assumption.1 および Assumption.3 の元, 健全性とリアルタイム無証拠性が両立する.

[**Proposition**]

$(\mathbb{G}_3, \mathbb{G}_2)$-Schnorr 認証において Assumption.2 および Assumption.4 の元, 健全性とリアルタイム無証拠性が両立する.

[**Proposition**]

$(\mathbb{G}_2, \mathbb{G}_1)$-Schnorr 認証において Fact.1 および Assumption.5 の元, 健全性はあるがリアルタイム無証拠性があるとは限らない.

[**定理**]

$(\mathbb{G}_2, \mathbb{G}_1)$-Schnorr 認証においてリアルタイム無証拠性はない.

[**証明**]

リアルタイム無証拠性問題のインスタンス

$$(g, y, R, \mathcal{C}, \mathcal{Z})$$

が与えられたとき,

$$\mathrm{e}(\mathcal{C}, y) \stackrel{?}{=} \mathrm{e}(\mathcal{G}, R\,\psi(\mathcal{Z})^{-1})$$

を出力する.

[**Remark**]

$(\mathbb{G}_2, \mathbb{G}_1)$-Schnorr 認証の健全性の証明で得られた $\mathcal{G}_0, \mathcal{G}_1$ は $\mathbb{G}_2$ を Revocable DDH Group[HSK05] と見なすと公開鍵 g, y に対する Revoke 鍵 に他ならない.

4 まとめと課題と謝辞

本研究では 認証プロトコルに於けるリアルタイム無証拠性の概念を定義し, Schnorr 認証において リアルタイム無証拠性 と 健全性を両立させる事が一見すると矛盾するように思われる事を示した. そして [SHUK03, SHUK04] の楕円曲線の設定を用い生成した bilinear group $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3$ について, その暗号学的な性質を分類し, これらを Schnorr 認証に用いた場合プロトコルにどのような影響をあたえるかを検討し, 次の結果を得た.

- 暗号学的構造をもつ群で Schnorr 認証を実装し健全性とリアルタイム無証拠性を両立させる事が可能である.
  いくつかの仮定の下 $(\mathbb{G}_3, \mathbb{G}_1)$-Schnorr 認証, $(\mathbb{G}_3, \mathbb{G}_2)$-Schnorr 認証において健全性とリアルタイム無証拠性が両立する.
- 構造を持った群でプロトコルを構成する場合は, 群の安全性は DDH 安全だけでは不十分である.
  $(\mathbb{G}_2, \mathbb{G}_1)$-Schnorr 認証において健全性はあるがリアルタイム無証拠性がない.

本研究の特殊な bilinear group は $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_3$ のどれか 2 つをプロトコルに利用する場合に特化して抽象化されている. しかしながら pairing は非常に強力な道具で, 特に $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_3$ のすべてを活用してプロトコルを構成する場合は実現できる機能がもっと増えると考えられる. 従って より現実に近い bilinear group のモデルを構築する事が今後必要である.

さらに本研究で用いた Assumption と他のよく研究されている Assumption (BDDH 等) の関係も明確にすべきである. 本研究での DDH 問題等の第一引数は 必ず特定された生成元となっている. 詳細な安全性の分類をするためにより一般の場合も検討する必要がある.

また本研究では, プロトコルをほとんど変更せず, 使用する巡回群に構造をもったモデルを導入する事によって, 元々の群の安全性を分割し, 一見 矛盾するように思われる安全性要件が両立できることを示した. 矛盾する要件が判定問題と計算問題に分かれる場合, ここで用いたテクニックは他の離散対数問題ベースのプロトコルにも応用可能かもしれない. 今後, こうした群のモデルを使ったプロトコルや UC 安全性への応用 [IA05] などを研究する必要がある.

本研究に関連して NTT の 藤崎英一郎 主任研究員に楕円曲線および pairing に関する議論に参加頂き, 貴重な意見を頂いた.

参考文献

[Sch91] C.P.Schnorr, "Efficient Signature Generation by Smart Cards," Journal of Cryptology, 4, 3, pp.161-174, 1991

[Oka93] T.Okamoto, "Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes," Proc. CRYPTO'92, LNCS 740, pp.31-53, Springer-Verlag, 1993

[FS86] A.Fiat, A.Shamir, "How to Prove Yourself: Practical Solution to Identification and Signature Problems," Proc. CRYPTO'86, LNCS 263, pp.186-194, Springer-Verlag, 1986

[SHUK03] T.Saito, F.Hoshino, S.Uchiyama, T. Kobayashi, "Candidate One-Way Functions on Non-Supersingular Elliptic Curves," Technical Report of IEICE. ISEC 2003-65 (2003-09)

[SHUK04] T.Saito, F.Hoshino, S.Uchiyama, T. Kobayashi, "Non-Supersingular Elliptic Curves for Pairing-Based Cryptosystems," IEICE Trans. Fundamentals, VOL.E87-A, NO.5, pp.1203-1205, May 2004

[HSK05] F.Hoshino, K.Suzuki, T.Kobayashi, "Revocable DDH by using pairing and it's application," Proc. SCIS2005, pp.1609-1612

[IA05] Y.IWASAKI, S.ARITA "A Universally Composable Commitment Protocol based on KEA1 and Revocable DDH Assumptions," IEICE Technical Report, ISEC2005-107, OIS2005-70(2005-11),pp.57-62, 2005