Schnorr 署名の理論安全性評価

研究年度　令和　4　年度
研究期間　令和　4　年度
研究代表者名　福光　正幸

はじめに

Schnorr 署名［Schnorr, 1991］は，代表的なディジタル署名（Digital Signature：データの所有者の認証とデータの改ざん検知を同時に行うことができる暗号技術）であり，その構造のシンプルさと処理効率の良さから，暗号資産の一種であるビットコインの中での利活用も検討されている［Bitcoin Forum］．Schnorr 署名の特徴の一つは，理論的安全性証明がされていることである．この安全性証明（Security Proof）とは，計算量的に解決困難（すなわち，スーパーコンピュータを含む実世界に存在するコンピュータを用いたとしても現実的な時間では解けない）と信じられている問題の解決困難性を仮定することで, 暗号技術の安全性を証明するフレームワークのことである. Schnorr 署名については，離散対数問題（Discrete Logarithm Problem）と呼ばれる著名な数論的な問題の解決困難性を仮定することで，安全性が証明されている［Pointcheval, Stern, 2000］.

一方，ビットコインの基盤技術であるブロックチェーンを用いる場合，大量ユーザの署名検証用の公開鍵が全ユーザに公開されることとなる. この場合, 安全性とデータ容量の効率性の観点から, 次の A), B)が保証されることが望ましい.

A)　大量ユーザの公開鍵が攻撃者に知られた状況においても安全であること.

B)　鍵や署名データの長さを決定するパラメータを短くしても安全であること.

A)について，EUF-CMA（Existential Unforgeability under Chosen-Message Attack）安全性と呼ばれる安全性を持つかどうかをディジタル署名の場合は一般的に議論されるが，この安全性では攻撃対象となる公開鍵が単一である場合のみしか想定されていない．これに対し，複数の公開鍵が攻撃対象として考慮された安全性を総称して「Multi-User Security」と呼び，EUF-CMA の Multi-user Security 版となる MU-EUF-CMA（Multi-User Existential Unforgeability under Chosen-Message Attack）は，Multi-user Security の中でも代表的な安全性定義として引用されている．実際，これまでに Schnorr 署名の MU-EUF-CMA 安全性について議論されてきた［Kiltz, Masny, Pan, 2016］．$\varepsilon \yen leq p \varepsilon'$

一方，暗号技術の鍵や署名データなどの長さを決定するパラメータは，仮定した問題の解決困難レベルに依存するが，B)の保証に関して，「緊密な安全性」と呼ばれる強い安全性が定義されている．緊密な安全性（Tight Security）は，安全性証明の際に構成する帰着アルゴリズム R に関する確率を用いて定義される．そもそも安全性証明では，証明対象の暗号方式の安全性を確率 ε で破る攻撃アルゴリズム A が存在すると仮定した場合，計算量的に解決困難と信じられている問題（例：素因数分解問題，離散対数問題，最短ベクトル問題）を確率 ε' で解決できるアルゴリズム R が構成できることを示す．緊密な安全性は，アルゴリズム R の解決確率 ε' とアルゴリズム A の攻撃成功確率 ε の割合 p が定数にできることをいう．例えば，緊密な安全性を持たず，p が多項式，すなわち，仮定した問題を解く確率 ε' の多項式倍の確率で暗号技術への攻撃が成功する場合，安全性維持のため，仮定した問題の推奨パラメー

タより暗号技術のパラメータをその多項式 p 分だけ長く設定しなければならない．つまり，鍵や署名データの長さを長くしなければ安全な運用が保証できない恐れがある．一方，緊密な安全性を有する暗号技術の場合，この割合が定数なので，仮定した問題の推奨パラメータと同程度のパラメータの長さであっても安全性を保証できる．すなわち，B)を保証していることになる．

Schnorr 署名の緊密な安全性について従来研究 [Paillier, Vergnaud, 2005] では証明困難とされていたが，近年，Fuchsbauer, Plouviez, Seurin [Fuchsbauer, Plouviez, Seurin, 2020] によって，Algebraic Group Model と呼ばれるセキュリティモデルに限定した場合，Schnorr 署名の緊密な EUF-CMA 安全性を達成できることが示された．しかし，この結果は，緊密な MU-EUF-CMA 安全性までは達成しておらず, A)と B)の保証を両立できるかどうかは未解決問題となっている. それどころか, Multi-User Security と Algebraic Group Model が両立できるかどうかは解明されていなかった.

研究内容・成果

そこで，本研究では Schnorr 署名の Multi-User Security と Algebraic Group Model の両立可能性を分析した．その結果として，Algebraic Group Model において，Schnorr 署名の MU-EUF-CMA 安全性が証明不可となる状況証拠を得た. つまり, 安全性証明の際に構成する帰着アルゴリズム R が Algebraic Algorithm と呼ばれる種類のアルゴリズムであり，攻撃対象となる複数の公開鍵の生成方法がある特定の表現に限定された場合，離散対数仮定より，Algebraic Group Model 上で MU-EUF-CMA 安全性を証明不可であることを示した.

この結果は，上述の条件の下，Schnorr 署名の MU-EUF-CMA 安全性を破る攻撃アルゴリズム A を用いて, 離散対数問題を解決する帰着アルゴリズム R が存在した場合, そもそもこのアルゴリズム A が存在せずとも離散対数問題が解決できてしまうことで示された. ここで条件とした Algebraic Algorithm とは，この種のアルゴリズムが計算する群 G の元はアルゴリズムに与えられた群の元にて生成される，すなわち，このアルゴリズムによる G の元は全て入力の群の元の線形和で記述できるもののことをいう. 本結果の場合，R が Algebraic Algorithm であることを条件としているため，R が生成する群の元は入力の線形和で表現できることになる. R は離散対数問題を解決するアルゴリズムなので, G の元として，生成元 g と離散対数問題のインスタンス y が与えられる. また, Schnorr 署名の公開鍵は G の元なので, MU-EUF-CMA 安全性の対象となる複数の公開鍵{pk}において, $\mathrm{pk} = \alpha g + \beta y$（$\alpha$, β は整数）と記述できることになる．この表現の下，さらに我々の結果では，これら公開鍵の表現が，$\beta = 1$ の場合に限定した．この鍵の表現は，Kiltz，Masny，Pan [Kiltz, Masny, Pan, 2016] の結果でも採用されている.

また，この結果を下に，Fuchsbauer，Plouviez，Seurin の通常の EUF-CMA 安全性を証明した帰着アルゴリズムについて考察した．本結果で示した公開鍵の表現は，彼らの帰着アルゴリズム内でも採用されていることがわかり，これが原因となり彼らの帰着アルゴリズムを MU-EUF-CMA 安全性の帰着アルゴリズムを自然に拡張しようとしても，確率評価の際に困難が生じることも解明した．以上の成果は，国際ワークショップ「13th International Workshop on Advances in Networking and Computing（WICS22)」にて発表し，国際ジャーナル「International Journal of Networking and Computing」への招待を受け，投稿中である.

おわりに

本研究では, Schnorr 署名の Multi-User Security と Algebraic Group Model の両立可能性を分析し，両立不可となる一種の状況証拠を与えた．具体的には，次の 2 条件がある場合，離散対数仮定から Schnorr 署名の MU-EUF-CMA 安全性を Algebraic Group Model 上で証明できないことを示した．

- 安全性証明の際に構成する帰着アルゴリズム R が Algebraic Algorithm である．
- MU-EUC-CMA 安全性の対象となる複数の公開鍵{pk}の表現が $\mathrm{pk} = \alpha g + y$ という形に限定されている．

また，この結果を基に，Algebraic Group Model 上で Schnorr 署名の緊密な EUF-CMA 安全性を達成できることを示した Fuchsbauer，Plouviez，Seurin の結果をなぜ MU-EUF-CMA 安全性の証明に自然に拡張することが困難であるかについても考察した．

以上の結果は，逆に，R が Algebraic Algorithm でない場合，または，対象とする公開鍵の表現が $\mathrm{pk} = \alpha g + \beta y (\beta \neq 1)$ の場合，安全性証明できる可能性があることを示唆している．そこで，今後は本研究結果を基に，Schnorr 署名の Multi-User Security と緊密な安全性の両立可能性について，更に分析していく．

参照文献

Bitcoin Forum. Status of Schnorr signatures and bulletproof. 参照先： Bitcoin Forum: https://bitcointalk.org/index.php?topic=5150967.0

Fuchsbauer, G., Plouviez, A., Seurin, Y. (2020). Blind Schnorr signatures and signed ElGamal encryption in the algebraic group model. EUROCRYPT 2020, (pp. 63–95).

Kiltz, E., Masny, D., Pan, J. (2016). Optimal security proofs for signatures from identification schemes. CRYPTO 2016, (pp. 33–61).

Paillier, P., Vergnaud, D. (2005). Discrete-log-based signatures may not be equivalent to discrete log. ASIACRYPT 2005, (pp. 1–20).

Pointcheval, D., Stern, J. (2000). Security arguments for digital signatures and blind signatures. Journal of Cryptology, 361–396.

Schnorr, C.P. (1991). Efficient signature generation by smart cards. Journal of Cryptology, 161–171.