Vol.2021-CSEC-93 No.6
Vol.2021-IOT-53 No.6
2021/5/13

ペアリングフリーな属性ベース署名の実効性の評価

安在 恭弥[1,a)]　穴田 啓晃

概要：本技報では，双線形群を用いない（ペアリングフリーな）離散対数ベースの属性ベース署名スキームの実効性を評価する．評価は 2016 年に Herranz が発表したスキームを対象とし，データサイズ及び計算量の漸近特性，及び，C 言語と OpenSSL ライブラリによる実装について行う．結果として，（属性ユニバースの位数やユーザーの設定最大数といった）パラメータの値が小さい場合は当該スキームは実効性があるものの，漸近的には実効性に乏しいと結論付ける．

キーワード：ディジタル署名，属性ベース，ペアリングフリー

Feasibility Evaluation of Pairing-Free Attribute-Based Signatures

Kyoya Anzai[1,a)]　Hiroaki Anada

Abstract: In this technibal report, we evaluate feasibility of an attribute-based signature scheme that is discrete-logarithm-based and that does not use bilinear groups (pairing free). The evaluation is on the scheme proposed by Herranz in 2016 about asymptotic behavior of data size and computational amount, and implementation by C language and the Open SSL library. As a result, we conclude that, though the scheme has some feasibility when the values of the parameters (such as the size of the attribute universe and the designed maximum of the number of users) are small, it does not have any effective feasibility asymptotically.

Keywords: digital signature, attribute-based, pairing free

1. はじめに

プライバシー保護の社会的要望を背景に，情報処理の実行者の匿名性が保証される暗号要素技術が盛んに研究開発されている．Maji ら [12], [13] により提案された属性ベース署名（Attribute-Based Signatures，以降 ABS）は，署名した主体の匿名性を保証するデジタル署名方式の一種である．属性ベース署名では，署名されるべき文書に対し署名ポリシーが付される．署名ポリシーとは，種々の属性で記述されたブール式である．例えば “部長職 AND (開発部門 OR 人事部門)” などである．ユーザーは，属性権限機関から発行された属性証明書を用い署名する．署名の検証者は，署名が正しく生成され，かつ，属性を各変数へ真とアサインした時のブール式全体の評価値が真となるときのみ署名を受理する．ABS では，悪意あるユーザーらが属性証明書を持ち寄り結託しても，署名を偽造することは計算量的にできない．

ABS の先行研究で広く知られたものには Maji ら [12], [13] や Okamoto-Takashima[14] がある．これらの先行研究の設計では，双線形群の性質 [14] が本質的に用いられている．双線形群とは，有限巡回群 $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ についての写像 $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ が双線形性と非退化性を満たすときに言う．双線形性とは，$\mathbb{G}_1, \mathbb{G}_2$ の任意の 2 点 P, Q 及び任意の整数 a, b に対し $e(P^a, Q^a) = e(P, Q)^{ab}$ となる性質である．非退化性とは，$e(P, Q) \neq 1_{\mathbb{G}_T}$，ただし $1_{\mathbb{G}_T}$ は $\mathbb{G}_T$ の単位限，となる $P \in \mathbb{G}_1, Q \in \mathbb{G}_2$ が存在する性質である．双線形群は，写像 e を有限体上の楕円曲線上のペアリング [9] として実現することで計算機実装可能となる．しかしながら，ペアリングとしての写像 e の計算時間は群 $\mathbb{G}_1$（あるい

[1] 長崎県立大学, 長崎県西彼杵郡長与町まなび野 1-1-1,
University of Nagasaki, 1-1-1 Manabino Nagayo-cho, Nishisonogi-gun, Nagasaki-ken
[a)] mc121001@sun.ac.jp

は $\mathbb{G}_2$）の内部の演算よりも数倍から 10 倍程度の計算時間を要する（[11]）．加えて，暗号要素技術の安全性の根拠となる，写像 e に対する計算量的な仮定が，関連する強力な攻撃法により見直しを迫られる可能性もある（[5] 等）．

双線形群を用いない ABS としては，巡回群 G の離散対数問題に基づき安全な Herranz のスキーム [10] が知られている．この ABS の設計は，知識のゼロ知識対話証明のシグマプロトコル [6] を Fiat-Shamir 変換 [8] したものである．ただし，monotone なブール式を取扱うためには OR プルーフ (OR-proof）の拡張を用いる [3], [4], [7]．この設計は，Maji ら [12], [13] や Okamoto-Takashima[14] の ABS の設計とは異なる方針と考えられ，特色あるものである．計算機実装の観点からは，ペアリングを用いない ABS を実現していると考えられる（以降「ペアリングフリーな ABS」）．ただし，Herranz のスキーム [10] はスキームのセットアップ時にユーザーの最大数を設定するという制約がある．

1.1 本研究の貢献

本技報では，ペアリングフリーかつ離散対数ベースの Herranz の ABS [10] について，上述の制約を踏まえ，理論的な漸近性能及び実装時の性能を評価する．実装はC言語と OpenSSL ライブラリ [1], [2] による．結果として，パラメータの値が小さい場合は当該スキームは実効性があるものの，漸近的には実効性に乏しいと結論付ける．

2. ペアリングフリーな属性ベース署名 [10]

本節では，次節以降でペアリングフリーな属性ベース署名スキーム（ABS）の実効性を評価するため，Herranz の ABS [10] のシンタックスを説明する．一般に，ABS は四つの確率的多項式時間アルゴリズムの組 $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Vrfy})$ であり，Herranz の ABS [10] もまたこれに従う．

$\mathsf{Setup}(1^\lambda) \to (\mathsf{pms}, \mathsf{msk})$．この確率的多項式時間アルゴリズムは，セキュリティパラメータ 1^λ を引数にとる．Setup はまずビット長 λ の素数 q を位数とする巡回群 $\mathbb{G} = \langle g \rangle$ を決定する．また，$H : \{0,1\}^* \to \mathbb{Z}_q$ なるハッシュ関数と，属性ユニバース $\tilde{\mathcal{P}} = \{\mathsf{at}_1, ..., \mathsf{at}_N\}$ を選択する．また，ユーザーの最大数を L とし，M を $M = L + N$ とおく．すべての $i \in \{1, ..., N\}$，$j \in \{1, ..., M\}$ に対して，巡回群 ${\mathbb{Z}_q}^*$ に含まれる元からランダムに $x_{i,j}$ を選び，$Y_{i,j} = g^{x_{i,j}}$ を計算する．追加する要素 h を $\mathbb{G}$ からランダムに決定し，公開鍵を含む公開パラメータ $\mathsf{pms} = (q, \mathbb{G}, g, h, H, \tilde{\mathcal{P}}, L, N, \{Y_{i,j}\}_{1 \le i \le N, 1 \le j \le M})$ 及びマスター秘密鍵 $\mathsf{msk} = (\{x_{i,j}\}_{1 \le i \le N, 1 \le j \le M})$ を出力する．

$\mathsf{KeyGen}(S, \mathsf{msk}, \mathsf{pms}) \to (\mathsf{sk}_S)$．この鍵生成アルゴリズムは，属性ユニバース $\tilde{\mathcal{P}}$ の部分集合である S，マスター秘密鍵 msk，及び公開パラメータ pms を引数に取る．$(\mathbb{Z}_q)^M$ の中からランダムにベクトル $a = (a_1, ..., a_M)$ を選択する．そして各 $\mathsf{at}_i \in S$ について，$s_i = \sum_{j=1}^{M} a_j x_{i,j} \bmod q$ を計算する．ただし，要素 s_i のいくつかが 0 になった場合 (それが起こるのはほぼ無視できる確率ではあるが)，新たにベクトル a を選択しなおす．よって，出力される個別秘密鍵 $\mathsf{sk}_S = (a, \{s_i\}_{\mathsf{at}_i \in S})$ は $\mathbb{Z}_q$ の要素を $M + |S|$ 個含む．受け手はすべての $\mathsf{at}_i \in S$ について $g^{s_i} = \prod_{j=1}^{M} {Y_{i,j}}^{a_j}$ が成り立っていることを確認することで正当に生成されたことを検証することができる．

$\mathsf{Sign}(m, \mathcal{P}, t, \mathsf{sk}_S, \mathsf{pms}) \to \sigma = (f(x), \{(A_i, u_i, \tilde{u}_i, z_i, \tilde{z}_i, e_i, \{w_{i,j}\}_{1 \le j \le M}\}_{1 \le i \le n}, \{w_j\}_{1 \le j \le M})$．この署名アルゴリズムは，メッセージ m，属性ユニバース $\tilde{\mathcal{P}}$ の部分集合である属性集合 $\mathcal{P}$，閾値 t[*1]，秘密鍵 $\mathsf{sk}_S = (a, \{s_i\}_{\mathsf{at}_i \in S})$ 及び公開パラメータ pms を引数とする．この署名アルゴリズムは，位数が丁度 t である S'，ただし $S' \subset S \cap \mathcal{P}$，を選択する．一般性を失わないようシンプルに表記するならば，$\mathcal{P} = \{\mathsf{at}_1, ..., \mathsf{at}_n\}$，$S' = \{\mathsf{at}_1, ..., \mathsf{at}_t\}$ としてもよい．ユーザーは以下の非対話型ゼロ知識証明プロトコルによって署名 σ を計算する．

まず，署名者が，安全性証明ではランダムオラクルと扱われるハッシュ関数 H を適用し c を得る（Fiat-Shamir 変換 [8]）．ここで，H の引数は命題 $x = (q, \mathbb{G}, g, h, \{Y_{i,j}{}_{1 \le i \le n, 1 \le j \le M}, \mathcal{P}, t)$，コミットメント $Cmt = (\{A_i, \tilde{A}_i, T_i, R_i, U_i)\}_{1 \le i \le n}$，及びメッセージ m である．Cmt の中身は以下のように定義する．$j = 1$ から M 及び $i = 1$ から n まで $r_i, \kappa_i, \delta_j \in_R \mathbb{Z}_q$ なる r_i, κ_i, δ_j をランダムに選び，$A_i = h^{r_i} \cdot \prod_{j=1}^{M} {Y_{i,j}}^{a}{}_j, T_i = h^{\kappa_i} \cdot \prod_{j=1}^{M} {Y_{i,j}}^{a}{}_j, T_i = h^{\delta_i}$ を計算する．$i = t+1$ から n について $c_i, u_i, \tilde{u}_i, z_i, \tilde{z}_i \in_R \mathbb{Z}_q$ をランダムに選択し，$i = t+1$ から n と $j = 1$ から M にかけて $w_{i,j} \in_R \mathbb{Z}_q$ を選び，$U_i = {A_i}^{-c_i} \cdot g^{u_i} \cdot h^{z_i}$，$\tilde{A}_i = {A_i}^{\tilde{u}_i} \cdot h^{-\tilde{z}_i} \cdot g^{-c_i}$，$R_i = {A_i}^{-c_i} \cdot h^{z_i} \cdot \prod_{j=1}^{M} {Y_{i,j}}^{w}{}_{i,j}$ を計算する．$i = 1$ から t については $\alpha_i, \beta_i, \tilde{\alpha}_i, \tilde{\beta}_i \in_R \mathbb{Z}_q$ を選び，$j = i$ から M について $\delta_{i,j} \in_R \mathbb{Z}_q$ を選び，$U_i = g^{\alpha_i} \cdot h^{\beta_i}$，$\tilde{A}_i = {A_i}^{\tilde{\alpha}_i} \cdot h^{-\tilde{\beta}_i}$，$R_i = h^{\beta_i} \cdot \prod_{j=1}^{M} {Y_{i,j}}^{\delta_{i,j}}$ を計算する．以上によって Cmt は定義されている．あるメッセージ m に署名し，m についての知識の署名 $Ans = (f(x), \{(u_i, \tilde{u}_i, z_i, \tilde{z}_i, e_i, \{w_{i,j}\}_{1 \le j \le M})\}_{1 \le i \le n}, \{w_j\}_{1 \le j \le M})$ がこのメッセージの署名となる．$f(x)$ はランダムに生成された c に対し，せいぜい $n - t$ 次式の多項式 $f(x) \in \mathbb{Z}_q[X]$ のなかで，$f(0) = c, f(i) = c_i$ となるようなものを計算する．ただし，$i = t+1, ..., n$ とする．$i = 1, ..., t$ に関しては $c_i = f(i)$ とし，$u_i = \alpha_i + c_i s_i, \tilde{u}_i = \tilde{\alpha}_i + c_i {s_i}^{-1}, z_i = \beta_i + c_i r_i, \tilde{z}_i = \tilde{\beta}_i + c_i r_i {s_i}^{-1}$ を計算する．$i = 1$ から t，及び $j = 1$ から M に関して $w_{i,j} = \delta_{i,j} + c_i a_j$ を計算する．$i = 1, ..., n$ に関して $e_i = \kappa_i + c r_i$ を，$j = 1, ..., M$ に関して $w_j = \delta_j + c a_j$ を計算する．

結果として，$\mathcal{P}$ のうちの t 個を用いることで $\sigma =$

[*1] 閾値ポリシーの場合．Monotone ポリシーは拡張することは可能である [3], [4], [7]

$(f(x), \{(A_i, u_i, \tilde{u}_i, z_i, \tilde{z}_i, e_i, \{w_{i,j}\}_{1\le j\le M}\}_{1\le i\le n}, \{w_j\}_{1\le j\le M})$ を出力する．

$\mathsf{Vrfy}(\sigma, m, \mathcal{P}, t, \mathsf{pms}) \to 1$ or 0．この検証アルゴリズムはメッセージ m，それに付随する署名 σ，署名ポリシーと閾値の組 $(\mathcal{P}, t)$ と，その署名ポリシー $\mathcal{P}$ に含まれる属性数 n，及び公開パラメータ pms を引数とする．検証者は以下の知識証明アルゴリズムに従って確認を行う．始めに，$f(x)$ の次数が最大で $n-t$ なのを確認する．次いで，すべての $\mathsf{at}_i \in \mathcal{P}$ について，$c_i = f(i)$ を計算し，$T_i = {A_i}^{-c} \cdot h^{e_i} \cdot \prod_{j=1}^{M} {Y_{i,j}}^{w_j}$, $R_i = {A_i}^{-c_i} \cdot h^{z_i} \cdot \prod_{j=1}^{M} {Y_{i,j}}^{w_{i,j}}$, $U_i = {A_i}^{-c_i} \cdot g^{u_i} \cdot h^{z_i}$，$\tilde{A}_i = {A_i}^{\tilde{u}_i} \cdot h^{-\tilde{z}_i} \cdot g^{-c_i}$ を計算する．もしも $f(0) = H(m, x, \{(A_i, \tilde{A}_i, T_i, R_i, U_i)\}_{\mathsf{at}_i \in \mathcal{P}})$ ならば 1 を，そうでないならば 0 を出力する．これによって $x = (g, h, \{Y_{i,j}\}_{1\le i\le n, 1\le j\le M}, \mathcal{P}, t)$ を示せた．これは 1-out-of-2 の OR-proof[7] を t-out-of-n に拡張した考え方である．

3. データサイズ及び計算量の漸近特性

本節では，ペアリングフリーな属性ベース署名スキームの一つである Herranz の ABS [10] について，データサイズ及び計算量の漸近特性を評価する．

比較の対象としては，双線形群を代数構造として用いる設計である Okamaoto-Takashima の ABS（PKC2011 [14], [15]）を採り上げた．その理由は，計算機実装する際にペアリングを用いると想定されていると考えられ，また，比較的多くの先行研究で引用されているからである．Okamoto-Takashima の ABS[14], [15] がよく引用されている背景には，安全性モデルが standard model であること，安全性仮定が DLIN（判定線形仮定 [14]）及び CR hash（衝突困難ハッシュ関数）であること，及び，扱える署名ポリシーが non-monotone であることが，優れた特徴として研究者に理解されている状況があるものと考える．なお，[15] のスキームのパラメータには属性ユニバースの設計自由度があるが，本技報では “sub-universe” の個数が一つの設定を想定した（単一のユニバース：[15] で “$d = 1$” に固定）．

ランダウの記号を O で表す．漸近特性の解析は，データサイズについては $|\mathsf{pms}|$, $|\mathsf{sk}_S|$, $|\sigma|$ について行った．一方，計算量については署名生成時間及び署名検証時間について行った．その理由は，現実に用いられる際に計算資源の乏しい可能性が高い署名生成及び署名検証の漸近特性を捉えるべきと考えたためである．他，安全性モデル，安全性仮定，扱える署名ポリシーを調査した．

結果を表 1 に示す．なお，有限体の四則演算についての 2 次以下の計算量，及び，ハッシュ関数の計算量は無視している

4. 実装評価

本節では，Herranz[10] の ABS について，計算機実装しアルゴリズムを実行したときの実行時間を評価する．計算機実装は複数のプログラムから成り立っており，各プログラムは上記 2 節で説明した Setup，KeyGen ，Sign ，Vrfy の 4 つである．

4.1 実装環境

実装環境は，ソフトウェアについては Linux（Ubuntu20.04.01LTS）上で C 言語を用いる．また，OpenSSL ライブラリ [1], [2] の一つとして楕円曲線ライブラリを ec.h で呼び出している．一方，ハードウェアについては，メモリ 16GB，コア数が 4 の CF-QV レッツノートを用いる．L はユーザーの最大数を，N は属性数を，n は署名ポリシー $\mathcal{P}$ に含まれる属性数を，t は署名ポリシー $\mathcal{P}$ を表す閾値をそれぞれ示す．

KeyGen は 10000 回動作する時間を，Sign 及び Vrfy は 100 回動作する時間を計測し，1 回あたりの時間を求めグラフ化する．

実験するパラメータ値はすべてユーザーの最大数を $L = 3$ で固定しており，それぞれのプログラムについて計算回数に影響のあるパラメータを動かして動作時間を計測するものとする．

4.2 実行時間

以下の折れ線グラフは，KeyGen，Sign，Vrfy の動作時間をグラフ化したものであり，縦軸はすべて単位は ms である．横軸は図 1 から図 3 までは $|S|$ を横軸とし，図 4，図 5，図 7，図 8 は N を横軸とし，図 6 及び図 9 は横軸を $n-t$ としたものである．

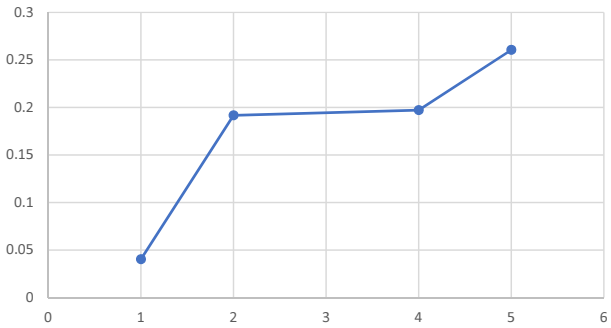

図 1 KeyGen の実行時間 1

5. 実効性の考察

本節では，データサイズ及び計算量の漸近特性，及び，実装評価について，ペアリングフリーな Herranz[10] の ABS スキームの実効性を考察する．

5.1 データサイズ及び計算量の漸近特性について

表 1 から読み取れることを以下に示す．

個別秘密鍵の長さ $|\mathsf{sk}_S|$，及び．署名長 $|\sigma|$ については，

表 1 属性ベース署名スキームのデータサイズの漸近特性

	Okamoto-Takashima[14]	Herranz[10]
$\lvert\mathsf{pms}\rvert$	$O(\lambda N^2)$	$O(\lambda N(L+N))$
$\lvert\mathsf{sk}_S\rvert$	$O(\lambda\lvert S\rvert)$	$O(\lambda\lvert S\rvert(L+N))$
$\lvert\sigma\rvert$	$O(\lambda n)$	$O(\lambda n(L+N))$
署名生成時間	$O(\lambda n)$	$O\big(\lambda(\alpha(n-t)^3+n(L+N))\big)$
署名検証時間 *1	$O(\lambda n)$	$O\big(\lambda(n(L+N))\big)$
安全性モデル	Standard model	Random oracle model
安全性仮定	DLIN and CR hash	DLOG and CR hash
署名ポリシー	Non-monotone	Monotone

記号の意味
λ: セキュリティパラメータ
L: ユーザーの最大数
N: 属性数
$|S|$: 個別秘密鍵の属性集合 S の位数
n: 署名ポリシー $\mathcal{P}$ に含まれる属性数
t: 署名ポリシー $\mathcal{P}$ を表す閾値
α: 和の第 1 項（ガウスの消去法）が第 2 項より計算量が少ないことを表す係数
*1) 署名検証では Okamoto-Takashima[14] の計算機実装ではペアリングの計算を要する
備考) 有限体の四則演算についての 2 次以下の計算量，及び，ハッシュ関数の計算量は無視している

表 2 Herranz[10] の属性ベース署名スキームの動作時間 (ms/回)

λ	256	512
Setup	136	440
KeyGen	0.3	0.4
Sign	469	1534
Vrfy	341	1132

パラメータの値は $L=3$, $N=10$, $|S|=3$, $n=10$, $t=3$.

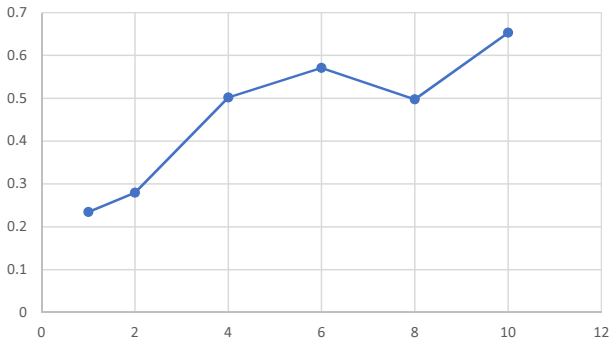

図 2 KeyGen の実行時間 2

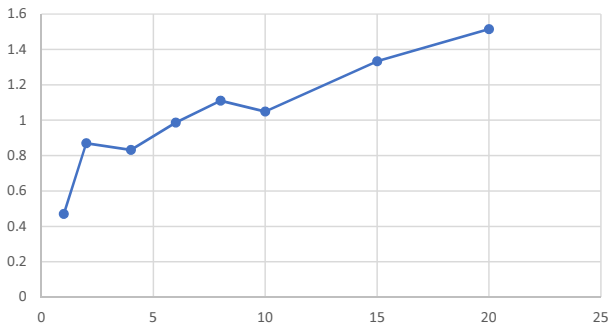

図 3 KeyGen の実行時間 3

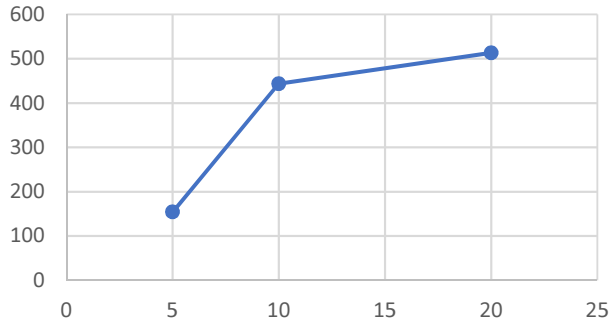

図 4　Sign の実行時間 1

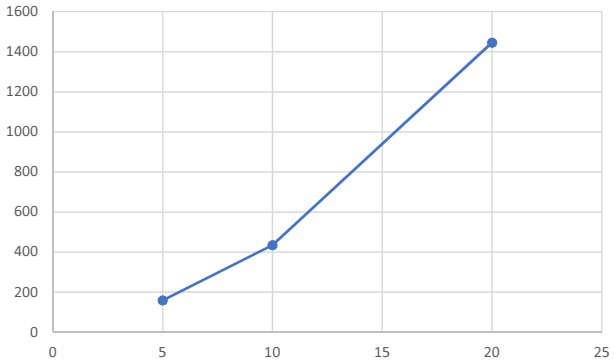

図 5　Sign の実行時間 2

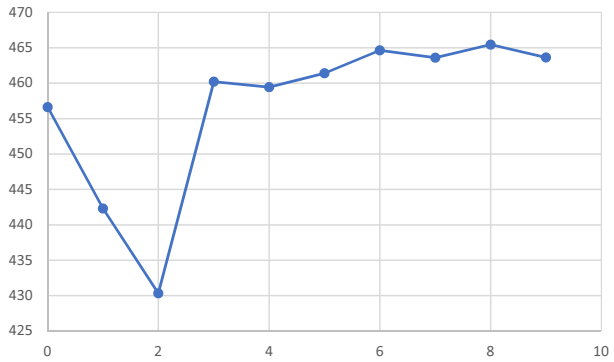

図 6　Sign の実行時間 3

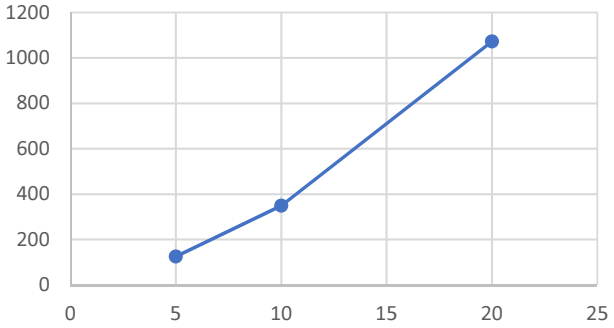

図 7　Vrfy の実行時間 1

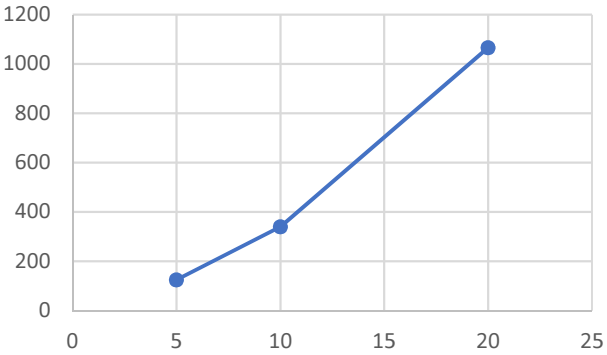

図 8　Vrfy の実行時間 2

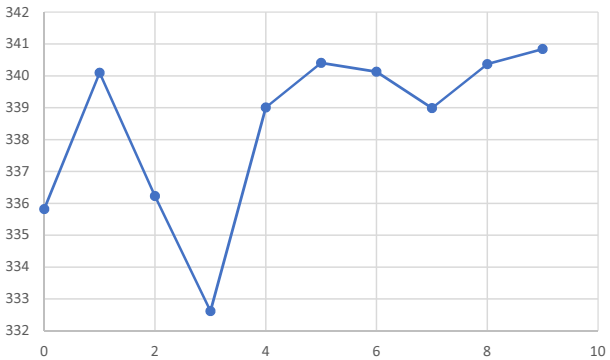

図 9　Vrfy の実行時間 3

Okamoto-Takashima[14] の ABS に比して Herranz[10] は「ユーザーの最大数＋属性数」の因子 $(L+N)$ の分だけ漸近的に大きい．署名生成時間，及び，署名検証時間についても，因子 $(L+N)$ の分だけ漸近的に大きい．ただし，署名検証では Okamoto-Takashima[14] の計算機実装ではペアリングの計算を要する．このため，漸近特性より精密な評価には定数係数の比較が必要である．

他，安全性モデルについては，Okamoto-Takashima[14] は standard model であるのに対し，Herranz[10] は random oracle model である．一方，安全性仮定については，Okamoto-Takashima[14] は DLIN（判定線形仮定），Herranz[10] は DLOG（離散対数仮定）であり，計算量的な困難さは DLOG 問題は DLIN 問題以上である．両問題の計算量理論的なギャップについては不明である．

以上から，少なくともデータサイズや計算量において優れているパラメータの値でないと，Herranz[10] の ABS スキームの方が Okamoto-Takashima[14] よりも実効性があることにはならない．

5.2 実装評価について

KeyGen，Sign，Vrfy それぞれのプログラムにおいて，計算回数はそれぞれあるパラメータに依存したループを持ち，計算オーダーはそのパラメータに依存したせいぜい多項式時間で表されると考えられる．KeyGen の計算には個別秘密鍵の属性集合 S の位数及びユーザーの最大数 L と N の合計値に依存したループがあり，計算時間は $|S|$ と $L+N$ に比例した関係になっていると考えられる．図 1，図 2，図 3 は KeyGen の実行時間のグラフであるが，それぞれ $N=5$，$N=10$，$N=20$ の時の横軸が $|S|$ となっている．$|S|$ については比例関係が見て取れ，N についても図 1 の $|S|=5$ の時の時間が，N が 4 倍となっている図 3 ではほぼ 4 倍になっているのが分かる．

Sign の計算には署名ポリシー $\mathcal{P}$ に含まれる属性数 n と閾値 t の差 $n-t$ にかかわる三重のループと，n 及びユーザーの最大数 L と N の合計値に依存したループがあり，その和に実行時間は依存していると考えられる．図 4，図 5 は $n-t$ をそれぞれ 2 と 3 に固定し，N を横軸としたグラフである．今回は N と n を同一の数値に設定しているため，実行時間は N の二次関数に依存しており，図 5 ではそれが顕著に見て取れる．図 6 は N を 10 で固定し，横軸を $n-t$ でとったグラフである．計算式上は計算時間は $n-t$ の三乗に依存するのだが，これによって計算回数の変わる逆行列を求める計算時間は非常に早く，計算時間自体にはほぼ影響を及ぼさない．よって，このグラフは測定上の誤差による上下を考慮すると数値上ほぼ横ばいで一定の値をとっている．

Vrfy の計算時間は Sign とほぼ同様のループに依存していると考えられる．実行時間グラフは Sign の図 4 と Vrfy の図 7 が，Sign の図 5 と Vrfy の図 8 が，Sign の図 6 と Vrfy の図 9 が対応しており，図 7 及び図 8 から Sign と同様にその計算時間は N について二乗に比例するとして問題はなさそうである．図 9 も図 6 と同様で，横軸は $n-t$ であるのだが，それによって影響される計算時間は微々たるもので，$n-t$ が 0 から 9 までの最大時間と最小時間の差は 10ms 以内と誤差としてもよい範囲内に収まっており，やはりこのグラフも Sign と同様にほぼ横ばいで，計算時間は $n-t$ にほぼ影響を受けないと見てよい．

なお，$L=3$，$N=10$，$|S|=3$，$n=3$，$t=3$ のケースで $\lambda=256$ と $\lambda=512$ についての動作時間を表 2 に示す．$\lambda=256$ については Sign と Vrfy の所要時間が 0.5 秒未満と現実的な値となった．

6. 結論

本技報では，ペアリングフリーな離散対数ベースの属性ベース署名スキームの実効性を評価する目的で，2016 年に Herranz が発表したスキームの漸近的性能及び計算機実装の性能を評価した．

今回の実装評価では，ユーザー数及び属性数が小規模ならば現実的な実行時間であろうことが分かった．一方，漸近的には実効性に乏しいと考える．留意点として，閾値ポリシーの場合，閾値 t による影響はごく軽微である．

今後の課題としては，属性数 N や個別秘密鍵の属性集合 S の位数がより大きくなった時に現実的に使用することができるかなどの調査や，具体的にどの程度の値ならばペアリングを用いた ABS スキームと比べてメリットがあるかを調査すること等である．

参考文献

[1] OpenSSL.
`https://www.openssl.org/`.
Accessed: 2020-8-1.

[2] 楕円曲線演算ライブラリ (openssl).
`https://sehermitage.web.fc2.com/etc/openssl_ec.html`.
Accessed: 2020-1-7.

[3] H. Anada, S. Arita, and K. Sakurai.
Attribute-based signatures without pairings via the fiat-shamir paradigm.
In *ASIAPKC'14, Proceedings of the 2nd ACM Workshop on ASIA Public-Key Cryptography, June 3, 2014, Kyoto, Japan*, pages 49–58, 2014.

[4] H. Anada, S. Arita, and K. Sakurai.
Proof of knowledge on monotone predicates and its application to attribute-based identifications and signatures.
IACR Cryptol. ePrint Arch., 2016:483, 2016.

[5] J. H. Cheon.
Security analysis of the strong diffie-hellman problem.
In S. Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, volume 4004 of *Lecture Notes in*

Computer Science, pages 1–11. Springer, 2006.

[6] R. Cramer.
Modular Designs of Secure, yet Practical Cyptographic Protocols.
PhD thesis, University of Amsterdam, Amsterdam, the Netherlands, 1996.

[7] R. Cramer, I. Damgård, and B. Schoenmakers.
Proofs of partial knowledge and simplified design of witness hiding protocols.
In Y. Desmedt, editor, *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings*, volume 839 of *Lecture Notes in Computer Science*, pages 174–187. Springer, 1994.

[8] A. Fiat and A. Shamir.
How to prove yourself: Practical solutions to identification and signature problems.
In *Advances in Cryptology - CRYPTO '86, Santa Barbara, California, USA, 1986, Proceedings*, pages 186–194, 1986.

[9] S. D. Galbraith, K. G. Paterson, and N. P. Smart.
Pairings for cryptographers.
Discrete Applied Mathematics, 156(16):3113–3121, 2008.

[10] J. Herranz.
Attribute-based versions of schnorr and elgamal.
Appl. Algebra Eng. Commun. Comput., 27(1):17–57, 2016.

[11] P. Longa.
High-Speed Elliptic Curve and Pairing-Based Cryptography.
PhD thesis, University of Waterloo, Ontario, Canada, 2011.

[12] H. K. Maji, M. Prabhakaran, and M. Rosulek.
Attribute-based signatures.
IACR Cryptol. ePrint Arch., 2010:595, 2010.

[13] H. K. Maji, M. Prabhakaran, and M. Rosulek.
Attribute-based signatures.
In *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, pages 376–392, 2011.

[14] T. Okamoto and K. Takashima.
Efficient attribute-based signatures for non-monotone predicates in the standard model.
In D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, editors, *Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings*, volume 6571 of *Lecture Notes in Computer Science*, pages 35–52. Springer, 2011.

[15] T. Okamoto and K. Takashima.
Efficient attribute-based signatures for non-monotone predicates in the standard model.
IACR Cryptol. ePrint Arch., 2011:700, 2011.