BGP 指向アグリゲート署名の構成

矢内 直人 † 千田 栄幸 ‡ 満保 雅浩 ⋆ 岡本 栄司 †

† 筑波大学 システム情報工学研究科
‡ 一関工業高等専門学校 電気工学科
⋆ 金沢大学 自然科学研究科

あらまし アグリゲート署名は個々の署名者に独立した文書に署名することを認める高機能暗号であり, その応用技術として BGP のセキュリティ強化が注目されている. 本稿では近年のアグリゲート署名と現実の BGP セキュリティには乖離があることを指摘する. この問題に対し, BGP を視野に入れた BGP 指向アグリゲート署名を提示する. その要件は (1) 署名が完全集約であること, (2) ID ベース暗号であること, (3) 一般型集約 ができることである. この要件のもとで既存方式を整理する. また, 最もこの条件に適する方式は Gentry-Ramzan であり, この方式を基に真に BGP に適した方式を構成する. 我々の予見では本方式は広大なネットワークエリアで実質上使用可能な唯一の方式である.

A Note on BGP-Aiding Aggregate Signatures

Naoto Yanai† Eikoh Chida‡ Masahiro Mambo⋆ Eiji Okamoto†

†Graduate School of Systems, and Information and Engineering, University of Tsukuba
‡Department of Electrical and Computer Engineering, Ichinoseki National College of Technology
⋆ Institute of Science and Engineering, Kanazawa University

Abstract Aggregate signatures are digital signatures which allow each signer to sign an individual document, and their application is for BGP security. In this paper, we pointed out a gap between state-of-the-art aggregate signature schemes and the recent BGP security, and describe BGP-aiding aggregate signatures which truly capture the BGP security. Their requirements are as follows: (1) full-aggregation, (2) ID-based cryptosystem, and (3) general aggregation. We look at the existing schemes under these observations. We identify that the Gentry-Ramzan scheme is the most suitable, and propose a truly suitable scheme by extending the scheme.

1 はじめに

現在のインターネットは自律システム (AS) と呼ばれる小規模なネットワークが相互に接続し合うことで構成され, この設計における近年の重要な課題の一つは AS 間のルーティング情報の保証である. YouTube Hijcaking [21] に代表されるように, border gateway protocol (BGP) [20] にて不正な AS パスの情報を伝達することで, 特定のネットワークへの到達性を失わせたり, 特定の Web サービスに対するすべてのトラフィックを盗聴できる [19]. これらの脅威を防ぐためには, 暗号技術の導入が求められており, 事実, 電子署名を用いた secure-border gateway protocol (S-BGP) [11] や border gateway protocol security extension (BGPSEC) [16] の標準化が IETF により進められている.

しかしながら, 暗号技術による負荷は無視できるものではない. 事実, 電子署名による負荷

により, ルータのメモリ負荷とパケット制約という新たな 2 つの問題が指摘されている. 前者の問題について, 現状の見積もりでは上述のプロトコルを導入するために必要なルータのメモリは数十ギガバイトにも上るが [23], このような高価なメモリを世界中の全ての機器に対して導入することは容易ではない. その一方, 後者の問題について, BGP のパケットサイズは最大で 4096 バイトであり [20], AS 間の経路情報, 各 AS の署名および公開鍵識別子などすべての情報をこのサイズに集約する必要がある [16]. 本稿では暗号学の観点からこの問題を鑑み, BGP に最適な高機能暗号を設計する.

実は現存する高機能暗号の中には既に BGP を視野に入れた暗号プリミティブが存在する. それがアグリゲート署名 [3] である. これは各署名者が個別のデータに署名でき, また, それらの署名を集約可能な技術である. 各ルータは自分の署名付き経路情報を従来技術よりもはるかに効率的に伝搬できるため, 暗号研究者の間ではアグリゲート署名は BGP を見据えた高機能暗号として注目されている [3, 4]. 本稿では近年の BGP 運用の観点から最新のアグリゲート署名の問題点を指摘する. 直観的には, 最新の方式が必ずしも BGP への応用に最良ではない. 本稿では BGP の機能を見つめなおすことで, アグリゲート署名が BGP に対して備えるべき姿, すなわち BGP 指向アグリゲート署名を議論する.

1.1 本稿の貢献

本稿では高機能暗号としてアグリゲート署名と BGP セキュリティの乖離問題を指摘し, また, BGP に対してアグリゲート署名が持つべき機能を提示する. その機能とはすなわち (1) 署名が完全に集約できること, (2) ID ベース暗号であること, (3) 一般型アグリゲート署名であることの 3 つである. この機能を備えた方式を BGP 指向アグリゲート署名と呼称し, 最新の理論研究との乖離を示す. 最後に, その具体的な構成として Modified-GR06 方式を構成する.

図 1: Update Message of BGP

2 BGP 及びその応用技術

本節では BGP と, その拡張機能を説明する.

2.1 Border Gateway Protocol

BGP は自ノードから宛先ノードまで AS 間の最短経路を動的に構成するプロトコルである. 各 AS は AS 番号 [9] と呼ばれる識別子と, その保有 IP アドレス空間を表す IP プレフィックスを有している. 各 AS 番号は IANA より地域インターネットレジストリ (RIR) に与えられ, RIR はそれらの番号を国別レジストリ (NIR) に, NIR は ISP に再帰的に割り当てていく.

プロトコルの詳細を以下に述べる. BGP ルータは隣接するルータとセッションを張り, 経路情報を update message として伝達する. update message の正確な構成は図 1 のようになっており, Path Attribute の中に IP プレフィックスと AS 経路情報が含まれる. AS 経路は AS 番号の連結として与えられる. この update message は通常 30 秒ごとの処理を設定している [20]. 同じ宛先 AS に対する最短経路が発見された場合は経路負荷を比較することで, 最短経路を動的に更新している. なお, update message の最大パケット長は 4096 バイトであり, このうち 19 バイトがヘッダ, 残りの 4073 バイトが可変長なパス情報空間として利用できる.

2.2 複数経路 (Multi-Path) BGP

近年の BGP では複数経路が重視されている [25]. その利点は, (1) ネットワークの容量拡充, (2) 経路更新に対するレスポンスの向上, (3) セキュリティの強化である. (1) について, 利用可能な経路を増やすことで負荷分散が可能となり, これによりトラフィックの増加が期待できる. (2) について, 単一経路では経路障害が発生した場合, 代替経路の構成に数分要することもありうる. しかしながら, 複数経路では遅延が数秒で済む [5]. また, (3) について, 敵は単一経路に対して攻撃を行うだけでは不十分であるため, 中間者攻撃への耐性向上と, 代替経路を通じた負荷分散による DoS 攻撃に対する頑強性が期待できる.

2.3 安全性の拡張

BGP では不正な情報を伝達することで特定 AS への到達性を失わせる脆弱性があった. そのため, S-BGP など経路情報の正当性を保証する技術が必要とされた. これらの技術では IP プレフィックスと AS 経路情報に電子署名を生成することで, その正当性を保証する. 現行の標準化動向としては, BGP の update message の Path Attribute の中に AS 番号, 公開鍵識別子, 署名からなる BGPSEC_path Attribute を挿入する形式で進められている [16]. これらの処理を繰り返し行うことで形成される.

これらの署名処理は RPKI [14] と呼ばれる専用の PKI を用いて実現される. その基本的な構成は従来の PKI と同様であり, 証明書自体の仕様は X.509 で与えられる. AS 番号と同様に IANA がリソース証明書を各 RIR に与え, 以下, その処理を末端まで繰り返す. 各 AS はこのリソース証明書の鍵を用いて署名する.

3 アグリゲート署名

アグリゲート署名は n 人の署名者に対してそれぞれ異なるデータに署名することを認め, またその署名サイズは高々ショート署名 1 個分に集約できる技術である [3]. これにより各ルータが個別に生成した署名の合計を高々1 個の署名として処理できるため, BGP が応用技術として注目されている. 事実, BGP にアグリゲート署名を導入することで, BGPSEC path Attribute は図 2(a) のように書ける. 従来技術にて問題点とされてきた署名長が固定長になることで, ルータのメモリの節約および多くの経路情報の伝達が可能になる. Zhao ら [26] は実際にアグリゲート署名を実装して, どの程度のパフォーマンス改善が得られるか評価も行っている. なお, 現存する方式は主に一般型アグリゲート署名 [3], 逐次型アグリゲート署名 [17], 同期型アグリゲート署名 [7, 1] の 3 つである.

一般型アグリゲート署名は Boneh ら [3] による最初のアグリゲート署名であり, これは確認が独立に生成した署名を集め, 任意のタイミングで集約する方式である. 直観的にはある種のブロードキャストを用いるため, 近年のアグリゲート署名の研究では敬遠されがちである. 逐次型アグリゲート署名 [17] は各署名者は署名処理と集約処理を同時に行う. これは一般型であったようなブロードキャストを避けることができるため, 効率的な運用ができることが知られている. また, 逐次型は署名と集約を同時に行うというある種の数学的興味を伴うため, 暗号研究者らの主たる興味は逐次型に向いている. 同期型アグリゲート署名は署名者間にてワンタイムな状態情報を同期することを前提とした方式であり, 署名の集約は同じ状態情報を持つ者だけが可能である. 同期型アグリゲート署名は効率的な署名を構成しやすいが, 一方で同期設定が不自然な仮定として敬遠されがちである.

4 アグリゲート署名と BGP の乖離

近年のアグリゲート署名は如何に逐次型処理を構成するかに特化している [4, 6, 8, 12, 13]. これは, 逐次型アグリゲート署名はブロードキャストを避けることでネットワーク全体の負荷を低下させることができること, また, 代数構造が複雑であり理論研究としての数学的興味が先行するためである. しかしながら, 逐次型アグリゲート署名は構成が難しい一方で, 近年の BGP

で採用されている複数経路のような並列構造において署名が集約できない問題がある．以下に，その詳細を説明する．まず，逐次型アグリゲート署名は署名とその集約を同時に行う．これは逐次型アグリゲート署名では署名を集約するためには秘密鍵が必要という見方ができる．ここで重要となる点は，並列構造では各署名者が独立してアルゴリズムを起動するため，署名が各経路において形成されることである．秘密鍵がないと集約処理ができないことから，各経路に対して署名を発行することは可能であっても，これら並列経路の署名を集約することは容易ではない．つまり，逐次型アグリゲート署名では集約が困難な署名が経路ごとに作成されてしまうため，複数経路に適さない．逐次型アグリゲート署名の署名と集約を同時に行う性質は署名の効率化および改ざん耐性に強い影響を与え，近年のアグリゲート署名の研究はこの逐次型アグリゲート署名の性質を如何に改善するかが中心となっている．不幸にも，高機能暗号の研究が数学的興味による理論を追求することに先行しすぎており，中核となるべき応用技術との乖離が発生していると言える．

その一方で，BGP に 対して求められることは署名長やパラメータサイズの縮小だけではない． これらの情報がどれほど小さいとしても，実際に伝送される情報は公開鍵識別子などの影響を受け，いずれパケットサイズ限界に達する．そのため，現実には署名長やパラメータサイズだけではなく，公開鍵識別子を含めた全体の情報量をいかに縮小するかが必須議論となる．

5 BGP 指向アグリゲート署名

本節ではアグリゲート署名が備えるべき機能について整理する． これらを満たした方式を BGP 指向アグリゲート署名と呼び，その具体的構成として Modified-GR06 方式を提案する．

5.1 BGP 指向アグリゲート署名の要件

5.1.1 完全集約

署名の圧縮効率は重要である．AS の数，すなわち署名者数は世界規模で見た場合，16-bit AS 番号で 65535，32-bit AS 番号で約 43 億個 にも上る．この台数は BGP のパケット制約を大幅に上回るため，署名長は人数に依存せず固定長になることが必須である．

5.1.2 ID-based Signature Scheme

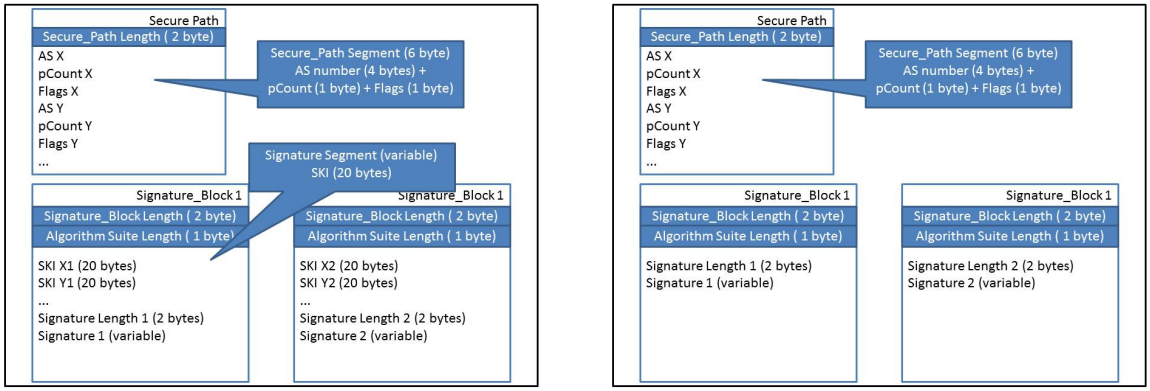
BGP のパケットサイズは 4096 バイトであり，仕様上，全てのデータはこの中に収まる必要がある．この中には公開鍵識別子も含まれる．公開鍵は乱数列で与えられ，従来の公開鍵暗号系システムではこの公開鍵識別子にて使用した公開鍵を表現している．公開鍵識別子の大きさは 20 バイトであり，従来の公開鍵暗号システムでは問題とならない．しかしながら，BGP の小さなパケット空間ではこれはボトルネックとなり，その除外は必須となる．高機能暗号としては，このような技術としては ID ベース暗号 [22] が知られている．これは任意のビット列を公開鍵として使用できる方式であり，例えば AS 番号を公開鍵として使うことが可能となる．これにより BGP パケットから公開鍵識別子を取り除き，図 2(b) のように構成することができる．

以下に，ID ベース暗号の BGP への応用について，運用面からの考察を述べる．ID ベース暗号の使用は現実世界ではしばしば証明書が不要となると誤解されがちである． しかしながら，公開鍵証明書は公開鍵および利用パラメータのデータフォーマットの規定するものであるため，鍵として任意の情報の利用可否に関わらず証明書の利用は通常は避けられない [10]．また，ID 自体に関しても，ID 情報とユーザの紐付けの保証も必要となる [18]．興味深いことに，BGP セキュリティではこれら ID ベース暗号の運用問題が BGP 自体の性質から解決できる．具体的には，BGP パケットという共通のデータフォーマットを用いることができること，また，AS 番号を公開鍵とすることで IANA への信頼を通じて公開鍵とユーザの紐付けもできることから，真に証明書が不要な運用が実現できる．これは BGP と ID ベース暗号が相互に欠点を不足し合うような親和性の高い技術であると言える．

表 1: 方式比較

提案方式の効率について比較する．$\mathcal{L}(p)$ は素数 p における群の元のサイズを，$L(N)$ は合成数 N における元のサイズを，k はセキュリティパラメータをそれぞれ表す．．

関連研究	署名長	ラウンド数	安全性仮定	経路	暗号系
BG10 [2]	$2L(N)+2k+\log n$	2	RSA	複数	IBC
BGLS03 [3]	$L(p)$	1	CDH	複数	PKI
GR06 [7]	$2L(p)+k$	1	CDH	複数	IBC
GLOW12 [8]	$5\mathcal{L}(N)$	-	CDH	単一	IBC
LLY13 [13]	$8\mathcal{L}(p)$	-	Static	単一	PKI
Modified GR06	$2L(p)+k$	CDH	CDH	複数	IBC



(a) PKI ベースアグリゲート署名　　(b) ID ベースアグリゲート署名

図 2: アグリゲート署名による BGPSEC_path Attribute の拡張

5.1.3　非対話な一般型集約処理

一般型集約処理は各署名者が個別に生成した署名をブロードキャストすることでアグリゲート署名を構成する手法である．これは最初のアグリゲート署名などが含まれるタイプであり，直観的には署名者間の対話処理を前提としている．一般に対話型処理は非効率であることから，近年のアグリゲート署名の研究では一般型集約処理を敬遠し，逐次型アグリゲート署名を採用している [4, 6, 12, 13]．その一方で，一般型集約処理は秘密鍵なしに署名を集約可能であるため，本質的な面で並列構造をサポートしている．すなわち，一般型集約処理が実は BGP security に最適といえる．

その一方，対話処理のラウンド数は現実世界で重要な意味を持つ．特に BGP では 30 秒ごとに update message を送信することが推奨されているため [20]，レスポンス向上させるためにはラウンド数を改善することが重要である．それゆえに非対話 (高々1 回のラウンド) であることが望ましい．

5.2　Modified-GR06 方式

本節では BGP 指向アグリゲート署名の具体的な構成を紹介する．これは GR06 方式を改良した方式であり，この方式を Modified-GR06 方式と呼称する．

5.2.1　GR06 方式の採用

既存方式の評価を表 1 にて与える．この表は ID ベースアグリゲート署名をまとめた内容である．この内容から GR06 方式を改良することで，

BGP 指向アグリゲート署名が構成できると判断した. 方式の詳細は次節以降で説明するが, この方式は同期型アグリゲート署名の一種である. 前述のとおり同期型設定は暗号研究では敬遠されがちだが, 実は現実世界においてはこの設定は実用的である [1]. 具体的には状態情報にはタイムスタンプを用いることができる. 例えば, タイムスタンプは BGP が動作する TCP/IP では 32 bit の空間を与えられパケットに取り入れられている. 一般にはタイムスタンプの同期が取れないパケットはリジェクトされるため, 同期型設定はむしろ現実的と言える.

その一方で, GR06 方式は同じ署名者の署名同士を集約する機能がない. これは複数経路における検証機能および精密な安全性解析に影響する. それゆえに, 我々は GR06 方式の改良が必要と判断した. 具体的には次節のグラフを定義し, このグラフ上の数学的性質を用いて方式を設計する.

5.2.2 直並列グラフ

本稿では以下の構造を用いて, Modified-GR06 方式を提案する.

直並列グラフの定義 $\mathcal{G}$ をグラフの集合とする. 直並列グラフは直列か並列のグラフを再帰的に定義することで構成される. 具体的には, 直並列グラフ $G(I,T)$ は始点 I と終点 T を用いて, 以下の通り定義される: $G(I,T)$ は以下のステップを繰り返すことで構成される.

1. $\mathcal{G}$ においてそれぞれ唯一なラベル i を伴い, $G_i(I_i,T_i)$ は I_i, T_i およびそれらを接続するエッジからなる. これを単グラフとする.
2. 以下のステップのいずれかを繰り返す.
   (並列) $1 \leq i \leq n$ において $G_i(I_i,T_i)$ を与えられ, $I = I_1 = I_2 = \cdots = I_n$, $T = T_1 = T_2 = \cdots = T_n$ とし, $G(I,T)$ とする.
   (直列) $1 \leq i \leq n$ において $G_i(I_i,T_i)$ を与えられ, $I = I_1, T_1 = I_2, \cdots, T_{n-1} = I_n$, $T_n = T$ とし, $G(I,T)$ とする.

グラフの合成 $\phi_1, \phi_2 \in \mathcal{G}$ におけるグラフの合成を並列において $\phi_1 \cup \phi_2$, 直列において $\phi_1 \cap \phi_2$ と定義する. ここで, $\mathcal{T}(i) = \{x \mid I_i = T_x \wedge 1 \leq x < i \wedge G_x(I_x,T_x) \subset \psi_n\}$ となる i 番目のグラフの始点の集合 $\mathcal{T}(i)$, $\mathcal{I}(i) = \{x \mid T_i = I_x \wedge i < x \leq n \wedge G_x(I_x,T_x) \subset \psi_n\}$ となる i 番目のグラフの終点となる集合 $\mathcal{I}(i)$ をそれぞれ定義する.

グラフの重み グラフの重み関数 $\omega_i(\psi_n)$ を定義する. $\omega_i(\psi_n)$ はインデックス i における I_i から T_n への経路数を表す. Tada [24] により, 直並列グラフにおける重みが解析されている.

5.2.3 方式構成

Modified-GR06 方式は同期型であり, ワンタイム情報 s の共有を仮定する. 前述のとおり s にはタイムスタンプを用いることができる.

Setup セキュリティパラメータ 1^k を与えられ, ペアリングパラメータ $(p, \mathbb{G}, \mathbb{G}_T, \boldsymbol{e})$, 生成元 $g \in \mathbb{G}$, 乱数 $\alpha \in \mathbb{Z}_p$ を生成する. その後, $A = g^\alpha$ を計算し, ハッシュ関数 $H_1 : \{0,1\}^* \times \{0,1\} \to \mathbb{G}$, $H_2 : \{0,1\}^* \to \mathbb{G}$, $H_3 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \to \mathbb{Z}_p^*$ を構成する. $(p, \mathbb{G}, \mathbb{G}_T, \boldsymbol{e}, g, A, H_1, H_2, H_3)$ をマスタ公開鍵, α をマスタ秘密鍵とする.

Key Generation 署名者の ID 情報 ID_i を与えられ, $j = \{0,1\}$ において $g_{i,j} = H_1(ID_i, j)$ および $g_{i,j}^\alpha$ を計算する. これらの値を ID_i の秘密鍵 sk_i として出力する.

Signing $(ID_i, m_i, \{\sigma_j\}_{j \in \mathcal{T}(i)}, \{\psi_j\}_{j \in \mathcal{T}(i)}, s)$ を与えられ, $g_s = H_2(s)$, $c_i = H_3(ID_i, m_i, s)$ を計算する. その後, 乱数 $r_i \leftarrow \mathbb{Z}_p$ を生成し, 以下を計算する:

$$S_i \leftarrow g_s^{r_i} g_{i,0}^\alpha (g_{i,1}^\alpha)^{c_i} \prod_{j \in \mathcal{T}(i)} S_j, \quad R_i \leftarrow g^{r_i} \prod_{j \in \mathcal{T}(i)} R_j.$$

Verification $(\{ID_j\}_{j \dot{\subset} \psi_n}, \{m_i\}_{i \dot{\subset} \psi_n}, \psi_n, s, \sigma_n)$ を与えられ, 以下を計算する:

$$\boldsymbol{e}(S,g) \stackrel{?}{=} \boldsymbol{e}(R, g_s) \boldsymbol{e}\left(A, \prod_{i=1}^{n} (g_{i,0}(g_{i,1})^{c_i})^{\omega_i(\psi_n)}\right),$$

ここで $g_s = H_2(s)$, $j \in \{0,1\}$ において $g_{i,j} = H_1(ID_i, j)$, $c_i = H_3(ID_i, m_i, s)$ を意味する. 検証式が成り立てば署名は正当, そうでないなら不当なものとする

5.2.4 安全性証明

本節では Modified-GR06 方式が CDH 仮定の下で安全であることを保証する. なお, 紙面の都合上, モデルおよび証明の詳細については省略する. 本証明は GR06 方式と同様に行える [7].

Theorem 1. $\mathbb{G}$ 上の (t', ϵ')-CDH 仮定かつランダムオラクル仮定が成り立つとする. このとき, 提案方式は $(t, q_s, q_k, q_{h_1}, q_{h_2}, q_{h_3}, n, \epsilon)$-secure である, ここで $t = t' - (5q_s + 2q_k + 2q_{h_1} + q_{h_2})\, t_e + \mathcal{O}(n)$, $\epsilon = \epsilon' \frac{e^3 \left(q_k + q_{h_1}(q_s + q_{h_3}) + 3\right)^3}{27}$, e は自然対数の底, t_e は一回のべき乗演算にかかる計算時間を意味する.

5.2.5 署名者数の制限

既存のグラフ理論の性質を活用すると提案方式の署名を偽造できる場合がある. 具体的には結託者の数が増加し, グラフの重み係数 $\omega_i(\psi_n)$ が 0 となる場合である. Tada は署名者数 n に対して $3^{n/3}$ が成り立つ限り, この攻撃は防げることを証明した [24]. ゆえに署名者数は $n = \frac{\log p}{\log 3} 3$ に制限される. 具体的には 80-bit security で 300 人, 128-bit security で 969 人程度である. これは一般型アグリゲート署名すべてに言える性質であり実運用上問題にならないこと, また, この制約を加味することで現実世界に利用できる方式は本方式だけであることを 6 節に述べる.

6 既存方式との実用性比較

我々の予見では一般型方式を複数経路に応用する場合, 前節の署名者数の制限を取り除くことは難しい. それゆえに提案方式だけでなく BG10 方式もまた, 同じ制約が生じる. 以降にて, この条件のもとで提案方式の考察を行う.

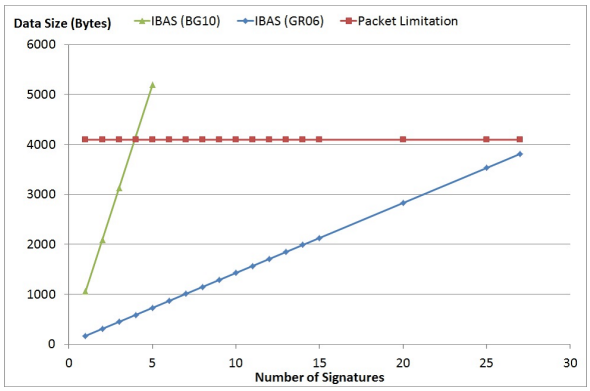


図 3: ID ベースアグリゲート署名の評価

16bit AS 番号では 65535 個の AS が存在している. しかしながら, 前述のとおり, 現実にはこれらの AS は IANA による一元管理ではなく, RIR が IANA より与えられた AS 番号を自身のネットワークにおいて再分配している. 実際の署名処理では, リソース public key infrastructure (RPKI) [14] を介して RIR が以下の組織に sub certificate と AS 番号を割り当てる. また, 実際の署名処理はこのリソース証明書のもとで実行される [15]. つまり, 現実には各 RIR にて形成される署名の総通信量が 4096 バイトより小さければ運用上の問題はない. 2013 年 5 月の段階において, 各 RIR が有する AS 番号の数は表 2 のとおりである [9].

128 bit security で見た場合, GR06 方式の最大人数は 969, BG10 の最大人数は 5814 である. これにより最大の RIR である ARIN 以下においては, GR06 方式では 27 個, BG10 方式では 5 個の署名が生成される. このときの通信量を表したものが図 3 である. この図から, BG10 方式はパケット限界を超過してしまうため, ARIN のような多くの AS を有する地域では使用できない. BGP の実用面を考えると, 提案方式だけが現実に使用可能と言える.

謝辞

本研究に関して有益なコメントをいただいた新・明るい暗号勉強会の皆さまに感謝する. 本研究はテレコム先端技術研究支援センターおよび JSPS A3 Foresight program によって支援されている. 彼らの支援に感謝する.

表 2: AS Numbers for each RIR

APNIC	ARIN	LACNIC	RIPE NCC	AfriNIC	IANA	未配布
7830	25428	3839	25112	1277	1042	1008

参考文献

[1] J. H. Ahn, M. Green, and S. Hohenberger. Synchronized aggregate signatures: New definitions, constructions and applications. In *Proc. of CCS 2010*, pages 473–484. ACM, 2010.

[2] A. Bagherzandi and S. Jarecki. Identity-based aggregate and multisignature schemes based on rsa. In *Proc. of PKC 2010*, volume 6056 of *LNCS*, pages 480–498. Springer, 2010.

[3] D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In *Proc. of EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 416–432. Springer, 2003.

[4] K. Brogle, S. Goldberg, and L. Reyzin. Sequential aggregate signatures with lazy verification from trapdoor permutations. In *Proc. of ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 663–680, 2012.

[5] A. de la Oliva, M. Bagnulo, A. Garcia-Martinez, and I. Soto. Performance analysis of the reachability protocol for ipv6 multihoming. In *Proc. of NEW2AN 2007*, volume 4712 of *LNCS*, pages 443–454. Springer, 2007.

[6] M. Fischlin, A. Lehmann, and D. Schrōder. History-free sequential aggregate signatures. In *Proc. of SCN 2012*, volume 7485 of *LNCS*, pages 113–130. Springer, 2012.

[7] C. Gentry and Z. Ramzan. Identity-based aggregate signatures. In *Proc. of PKC 2006*, volume 3958 of *LNCS*, pages 257–273. Springer, 2006.

[8] M. Gerbush, A. Lewko, A. O'Neill, and B. Waters. Dual form signatures: An approach for proving security from static assumptions. In *Proc. of ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 25–42. Springer, 2012.

[9] IANA. Autonomous system (as) numbers, 2013. `http://www.iana.org/assignments/as-numbers/as-numbers.xhtml`.

[10] A. Kanaoka, M. Okada, Y. Katsuno, and E. Okamoto. Probabilistic packet marking method considering topology property for efficiency re-building dos attack paths. *TIPSJ*, 52(3):929–939, 2011.

[11] S. Kent, C. Lynn, and K. Seo. Secure border gateway protocol. *IEEE Journal of Selected Areas in Communications*, 18(4):582–592, 2000.

[12] K. Lee, D. H. Lee, and M. Yung. Aggregating cl signatures revisited: Extended functionality and better efficiency. In *Proc. of FC 2013*. Springer, 2013. Available in `http://fc13.ifca.ai/proc/5-2.pdf`.

[13] K. Lee, D. H. Lee, and M. Yung. Sequential aggregate signatures with short public keys: Design, analysis and implementation studies. In *Proc. of PKC 2013*, volume 7778 of *LNCS*, pages 423–442. Springer, 2013.

[14] M. Lepinski. An infrastructure to support secure internet routing, 2012. RFC 6480.

[15] M. Lepinski. Bgpsec protocol specification, 2013. Internet Draft, `http://datatracker.ietf.org/doc/draft-ietf-sidr-bgpsec-protocol/`.

[16] M. Lepinski and S. Turner. An overview of bgpsec, 2011. Internet Draft, `http://tools.ietf.org/html/draft-ietf-sidr-bgpsec-overview-01`.

[17] A. Lysyanskaya, S. Micali, L. Reyzin, and H. Shacham. Sequential aggregate signatures from trapdoor permutations. In *Proc. of EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 74–90. Springer, 2004.

[18] K. G. Paterson and G. Price. A comparison between traditional public key infrastructures and identity-based cryptography. *Information Security Technical Report*, 8(3):57–72, 2003.

[19] A. Pilosov and T. Kapela. Stealing the internet - an internet-scale man in the middle attack, 2008. Defcon 16.

[20] Y. Rekhter and T. Li. A border gateway protocol 4 (bgp-4), March 1995. RFC 1771, `http://www.ietf.org/rfc/rfc1771.txt`.

[21] RIPE. Youtube hijacking: A ripe ncc ris case study, 2008. `http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study`.

[22] A. Shamir. Identity-based cryptosystems and signature schemes. In *Proc. CRYPTO 1984*, volume 196 of *LNCS*, pages 47–53. Springer, 1987.

[23] K. Sriram, O. Borchert, O. Kim, D. Cooper, and D. Montgomery. Rib size estimation for bgpsec, 2011. `http://www.antd.nist.gov/~ksriram/BGPSEC_RIB_Estimation.pdf`.

[24] M. Tada. A secure multisignature scheme with signing order verifiability. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E86-A(1):73–88, 2003.

[25] F. Valera, I. V. Beijnum, A. Garcia-Martinez, and M. Bagnulo. *Multi-Path BGP: Motivations and Solutions*, chapter 1, pages 238–256. Cambridge University Press, 2011.

[26] M. Zhao, S. Smith, and D. Nicol. Aggregated path authentication for efficient bgp security. In *Proc. of CCS 2005*, pages 128–138. ACM, November 2005.