ed25519のすすめ

Kazunori Fujiwara, JPRS
fujiwara@jprs.co.jp
2018/6/27

まとめとURLなど

- ED25519は3072ビットRSAと同程度の暗号強度であるにもかかわらず、公開鍵・署名サイズが非常に小さいため、DNSSECのパケットサイズ問題を改善できる。(フラグメントなし運用しやすい)
- ED25519の実装が進んできているので、みんなで遊びましょう。
- 関連資料など
  - https://ed25519.cr.yp.to
  - https://www.openssl.org
  - https://www.isc.org/git/
  - https://git.nlnetlabs.nl/ldns/
  - https://www.unbound.net/

DNSSECアルゴリズム

DNSKEYアルゴリズム		署名	ハッシュ	RFC	発行月	状況
5	RSASHA1	RSA	SHA1	3110	2001年5月	SHA1は脆弱
7	RSASHA1-NSEC3-SHA1	RSA	SHA1	5155	2008年3月	SHA1は脆弱
8	RSASHA256	RSA	SHA256	5702	2009年10月	現在の主流
10	RSASHA512	RSA	SHA512	5702	2009年10月	
12	ECC-GOST	ECC-GOST	GOST?	5933	2010年7月	GOST(旧版)
13	ECDSAP256SHA256	ECDSAP256	SHA256	6605	2012年4月	現在の主流
14	ECDSAP384SHA384	ECDSAP384	SHA384	6605	2012年4月	
15	ED25519	Ed25519	(SHA512)	8080	2017年2月	期待
16	ED448	Ed448	(SHAKE512)	8080	2017年2月	期待

Ed25519の概要

- アルゴリズムの提案者: Daniel J. Bernstein (DJB)
- エドワーズ曲線デジタル署名アルゴリズム(EdDSA)の一つ
- https://ed25519.cr.yp.to/ より
  - 高速な署名: 109000/sec (DJBのソフト, 4core 2.4GHz Nehalem)
  - 高速な検証: 71000/sec (DJBのソフト, 4core 2.4GHz Nehalem)
  - 2^128の暗号強度 … RSA 3072ビット, ECDSAP256相当
  - 署名サイズ: 64バイト　　(RSA 3072ビットだと384バイト)
  - 公開鍵サイズ: 32バイト　　(RSA 3072ビットだと384バイト)
- Ed25519は、OpenSSH, GnuPGなどで普及
- Ed448: Ed25519より暗号強度が高いEdDSA

署名アルゴリズムの比較

署名アルゴリズム	暗号強度	公開鍵サイズ	署名サイズ	ldns実行時間（秒）20005 RRset 署名・検証	
	bit	バイト	バイト	signzone	verify-zone
RSA 1024bit	≦80	128	128	5.00	2.13
RSA 2048bit	112	256	256	26.92	3.04
RSA 3072bit	128	384	384	75.92	3.98
ECDSAP256	128	64	64	2.72	4.59
ECDSAP384	192	96	96	33.95	23.72
Ed25519	128	32	64	2.77	5.30
Ed448	224	57	114	5.33	14.46

現在は112ビットから128ビットの暗号強度が求められている。
そのなかではEd25519の公開鍵サイズが最も小さく、ECDSAP256, Ed25519の署名が最も小さい。ECDSAP256とEd25519の署名時間は短く、検証時間もRSAより若干長い程度である。
暗号強度はNIST SP800-57、RFC 8032より
ldns実行時間は、10000の委任のみ、DSあり、署名、検証それぞれ20005 RR。テストマシンはXeon E5-2430v2、ldnsはマルチスレッド非対応

例: RSA 2048ビット

```
% drill -o rd -D @a.root-servers.net . dnskey
.       172800  IN      DNSKEY  256 3 8
AwEAAdU4aKlDgEpXWWpH5aXHJZI1Vm9Cm42mGAsqkz3akFctS6zsZHC3pNNMug99fKa7OW+tRHIwZEc//mX8Jt6bcw5bP
gRHG6u2eT8vUpbXDPVs1ICGR6FhlwFWEOyxbIIiDfd7Eq6eALk5RNcauyE+/ZP+VdrhWZDeEWZRrPBLjByBWTHl+v/f+xvTJ3
Stcq2tEqnzS2CCOr6RTJepprYhu+5Yl6aRZmEVBK27WCW1Zrk1LekJvJXfcyKSKk19C5M5JWX58px6nB1IS0pMs6aCIK2yaQ
QVNUEg9XyQzBSv/rMxVNNy3VAqOjvh+OASpLMm4GECbSSe8jtjwG0I78sfMZc= ;{id = 39570 (zsk), size = 2048b}
.       172800  IN      DNSKEY  257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g
0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz
1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu+ipAdT
TJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0= ;{id = 19036 (ksk), size = 2048b}
.       172800  IN      DNSKEY  257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+
B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9t
arpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8HF
Rm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU= ;{id = 20326 (ksk), size = 2048b}
.       172800  IN      RRSIG   DNSKEY 8 0 172800 20180701000000 20180610000000 19036 .
jYaHF5M9YJalkqEYRmdAt/n5brZG2GLGxgVxmXvV3Ls2hwjd9hUmOZ+DjB1imtI2l7WcDI4B0YVBKd09uUsD+fJSEg8bVpIjyUg
VAWgz0vMEuwIoz/dNNNm61Uj4uHv5tSoeDv5WiN2RLZ+eLZ9qQYN2G3kg6pk2ANbMGiO+OKGR1n254ZcAcekbIUBhr8PW1
re2vmNE3s9BYf+Jv606awQyWA6FByUeWJTR3r+LDRyFLpAEg1gb45zRHRGLm+Ut0jEiPs8BHRZ/eNcRU+Ir0zMvjlP5O4I9Vz
NFBZTZuvMp16X0/sBFzbjBBzrcxlaO4jpfDy9Bmq9YfJeSt+tTHg==
;; MSG SIZE  rcvd: 1139
```

例: ED25519

```
% drill -o rd -D @h.fujiwara.asia fujiwara.asia dnskey

fujiwara.asia.  3600    IN      DNSKEY  256 3 15
tCC9iJ85PJOEuSWoe5Ye+7BsGwq411Z6tG09EvtOMNc= ;{id = 36583
(zsk), size = 0b}
fujiwara.asia.  3600    IN      DNSKEY  257 3 15
NbWeEEDkeY1HTnkkBJXpQ9vuFH/yUTMIY7u6kxillyQ= ;{id = 45171
(ksk), size = 0b}
fujiwara.asia.  3600    IN      RRSIG   DNSKEY 15 2 3600
20180719180201 20180619160201 45171 fujiwara.asia.
Q68z3FtEFY8aDKs8m/mKRT58fjIswvA7N1QTFXwdtlM4J2v6Pr3iR4by
9I83UW2z/H5P2Oo2bVz0702qFWoiDw==
;; MSG SIZE  rcvd: 247
```

例: ECDSAP256SHA256

```
% drill -o rd -D @h.pyon.org pyon.org dnskey
pyon.org.       300     IN      DNSKEY  256 3 13
uqgw2ue9fPBzQwApWY+hQuG/j8F5JFyaxDgFBrSYX2lVpzI5btbQBJ9
C5FS/2Qh2CyjtZCks4Y7pz06p3VretQ== ;{id = 61810 (zsk), size =
256b}
pyon.org.       300     IN      DNSKEY  257 3 13
BxpjVKz+8eEGsd71JVAJr0NbPE63Ya+bHz1PtwWtNKVlplJgjCIcCIv+d
nfI0+JNmWMFFBHNg/SueKU4yzcRPA== ;{id = 9240 (ksk), size =
256b}
pyon.org.       300     IN      RRSIG   DNSKEY 13 2 300
20180719180201 20180619160201 9240 pyon.org.
fECSAnOVGbdw0nEjEdbtiG1g1IJG7HBLdAfVaStBRRnvzMI3K8emUo
mZa1o4wXBSSQ+RYHDl6ApXUvAhmqvFYw==
;; MSG SIZE  rcvd: 301
```

RSAの公開鍵・署名サイズが大きくなる理由

- RSAの公開鍵は、素数の積であるpqと、d=65537
  - RSAのビット数はpqの大きさ
  - 素数は自然数空間のごく一部なので、3072ビットあってもとりうるpqの組み合わせは少ないため、公開鍵の個数は少ない
  - 署名は、pqで割った余りなので、pqと同じ大きさ

- その点EdDSAでは、秘密鍵サイズ分の個数のキーあり
  - Ed25519 keygen は、32バイトの乱数生成… 2^256個の秘密鍵
  - Ed25519公開鍵は秘密鍵のSHA512下位32ビット (若干整形)

Signerの対応状況

- BIND 9, LDNSのみ評価
  - OpenSSL 1.1.1 (-pre6以降) が必要
  - BIND (9.12.1, 9.13, master): ED25519 対応, ED448バグあり
  - ldns (git master): ED25519, ED448対応
- 開発者からの情報 (dns-operations mailing list)
  - Knot DNS serverのsigner: ED25519対応
  - PowerDNS v4.0.x, v4.1.x: ED25519, ED448対応

Validatorの対応状況

- BIND 9, Unboundのみ評価
  - OpenSSL 1.1.1 (-pre6以降) が必要
  - BIND 9.12.1: ED25519/ED448バグあり
  - BIND 9 (9.13.0, git master): ED25519対応/ED448バグあり(servfail)
  - Unbound 1.7.1～ ED25519, ED448対応
- 1(ED25519対応), 8(非対応), 9(半分対応)
- 開発者からの情報 (dns-operations mailing list)
  - Knot resolver: ED25519対応
  - PowerDNS recursor v4.1.x: ED25519, ED448対応
- 知らないアルゴリズムに対しては、DNSSEC未署名と同じ動作
  - 検証しない, ad=0応答

レジストリ･レジストラの対応

- アルゴリズム15 (ED25519),16 (ED448)を指定できた組合せ
  - .ASIA, Doレジ (ファーストサーバ)
- アルゴリズム13 (ECDSAP256SHA256)を指定できた組合せ
  - .ORG,　GoDaddy
  - (多くのTLD, Registrarが対応しているはず)
- dns-operations mailing listで聞いた情報
  - .nl, .cz, .ch, .li はアルゴリズム15(ED25519) を受け付ける
  - 例: ed25519.nl, ed25519.cz

ソフトウェアのインストール

- OpenSSL 1.1.1 (-pre8) を先にインストール (/usr/local)
  - ./config; make; make install
- LDNS
  - 要: libtool 最新/2.4.6, autoconf 新しめ automake 新しめ
  - git clone https://git.nlnetlabs.nl/ldns/
  - autoreconf -i; ./configure --enable-ed25519 --enable-ed448 --with-drill --with-examples; make; make install
- Unbound 1.7.3
  - ./configure --with-openssl=/usr/local; make; make install
- BIND 9.13.0
  - ./configure --with-openssl=/usr/local --with-eddsa; make; make -k install

具体的な使い方

- dnssec-keygen, ldns-keygenでアルゴリズムとしてED25519を指定するだけ
  - dnssec-keygen **-a ED25519** [-f ksk] ドメイン名
  - ldns-keygen **-a ED25519** [-k] ドメイン名

まとめとURLなど

- ED25519は3072ビットRSAと同程度の暗号強度であるにもかかわらず、公開鍵・署名サイズが非常に小さいため、DNSSECのパケットサイズ問題を改善できる。(フラグメントなし運用しやすい)
- ED25519の実装が進んできているので、みんなで遊びましょう。
- 関連資料など
  - https://ed25519.cr.yp.to
  - https://www.openssl.org
  - https://www.isc.org/git/
  - https://git.nlnetlabs.nl/ldns/
  - https://www.unbound.net/