【2006/最終】プロジェクトNO.15・セキュリティパラダイムの革命 ―ペアリング暗号―・担当教員名

高木　剛/Takagi Tsuyosi
宮本衛市/Miyamoto Eiiti
小西　修/Konisi Osamu

セキュリティパラダイムの革命 ―ペアリング暗号―

Revolution of Security Technology – Pairing Based Crypto system

鈴木　康広 / Suzuki Yasuhiro　　仁科　五月 / Nishina Satsuki　　山端　亮輔 / Yamahata Ryousuke　　鳴海　寛之 / Narumi Hiroyuki　　石黒　司 / Ishiguro Tsukasa

片山　貴充 / Katayama　Takamitu　　林　卓也 / Hayashi Takuya　　阿部　勇介 / Abe Yuusuke　　能戸　幸雄 / Noto Yukio　　小松　康平 / Komatu Kouhei　　信田　寿広 / Nobuta Toshihiro

short signatureの概要 Abstract

short signatureとは文字通り「短い暗号」である。私たちは通信を用いる時、ディジタル署名によって通信の確実性や安全性について管理、照合しているわけだが、short signatureとはそのディジタル署名をペアリング暗号によって短くし、使いやすい形にするというものである。

Outline: Short Signature is literally ″short cipher″. When we use Broadcast, we control and collate about Safety or Certainty of communication by digital signatures. Then Short Signature is the digital signature which is useful and short style by using pairing encryptosystem.

short signatureの利点とは

利点：言わば、ディジタル署名とは私たちの生活の中における印鑑の捺印やサインに相当するものである。その署名自体がとても大きい物だと、どうだろうか？その署名を利用できる媒体は限られ、とても使いづらい物になってしまう。安全性を保持した上で、署名が小さければ色々な媒体で使う事が可能になる。

Advantage point : So to speak, digital signatures are equivalent to the sign or the sealing of a seal in our life. If the signature in itself is too big thing, media which is usable the signature is limited and it is hard to use. it is possible to use various media if the signature is short one and keep safety.

今までは、これだけ長かった

30 81 89 02 81 81 00 c6 8b a6 67 0e ce 63
dd 91 54 40 44 09 78 1a 81 54 84 8a a1 c4
8b 57 23 81 22 9a 89 1c aa cd e4 8e c6 c8 2f
06 e1 79 4e ae 79 e1 bf 46 0a 21 b1 be 62 11
0f 93 43 90 e6 c6 77 b2 2f ee 19 2b b3 69 08
04 65 6e 62 53 15 ff 53 19 27 33 83 62 53
f8 6a 19 d3 7a c6 41 78 2a db 84 50 e3 7d 44
04 c2 8c 0d 5a 7d

それが…

これだけ短くなる！

01 ab 20 e4 1a e0 05 cb b7 45
bb 8d e2 fc d4 f6 17 39 9c 48

高速化の概要 Abstract

ペアリング暗号には、従来の公開鍵暗号方式に比べ、暗号化・復号化にかかる時間が長いという欠点がある。そこで、様々な手法を用いて、ペアリング演算の高速化を図ることで、この欠点を克服する。

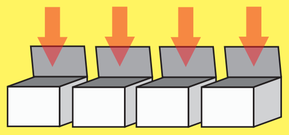
There is a weak point which the time encryption and decryption do take long time.Therefore we overcome by using various way which make pairing processing speed more high speed.

高速化の手法 How To Be Speedy

算術演算を用いた場合、1つの変数には1個の要素しか入れることが出来ず、また要素を1つずつしか計算出来ない。しかし、論理演算を用いると、2つの変数で32個の要素を入れることが出来、また32個ごと計算出来る。そのため、論理演算は算術演算より高速に計算出来る。

In case of using arithmetical process, one variable can only use one element and also it only calculate one element by one processing. However if it uses bit process, it can substitute thirty two elements to two variables, and also it can calculate thirty two elements by one processing. It is reason why bit processing can calculate faster than arithmetical process.

・GF(q) $q=3^{97}$の表現
↓
1　0　1　2　…



…

1個の箱に1個の要素！
97個の箱が必要！
（算術演算）

＊算術演算とは…
普段計算する時に使う
＋、－、×、÷
を用いた計算方法

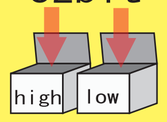
そこで…

highとlowの２つペアで
0,1,2を表現する
↓
例えば、

high	low	値
0	0	0
0	1	1
1	0	2

すると…

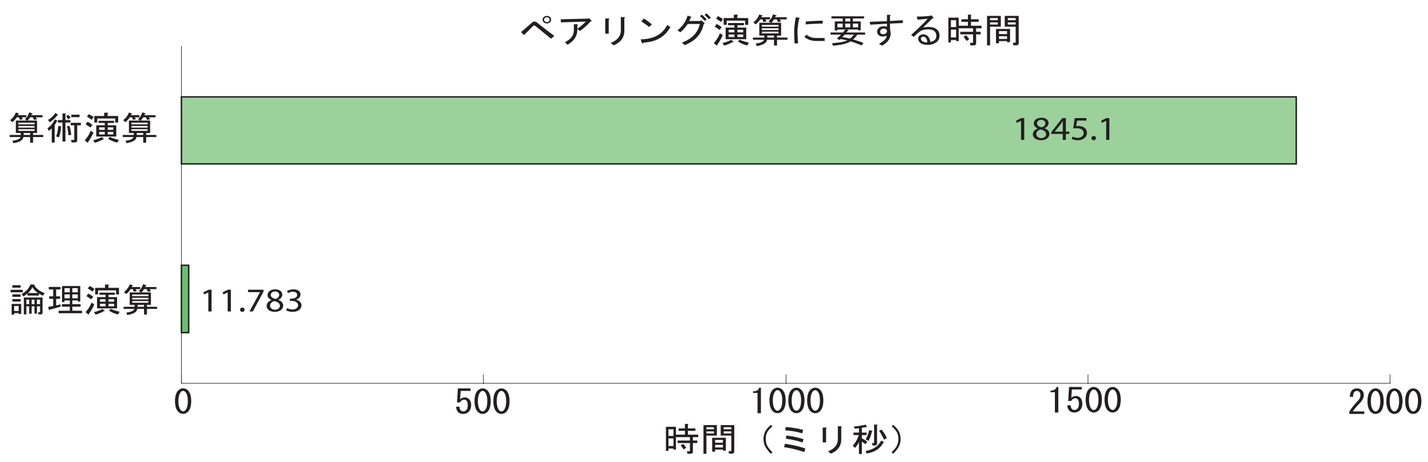
・GF(q) $q=3^{97}$の表現
↓
high 10010000010010000100100000100011…
low 00100001000100100010010011010100…
32bit



high, lowの2個の箱に32個の要素！
high4個, low4個の計8個で充分！
（論理演算）
↓
演算よりも高速
演算が可能！

＊論理演算とは…
コンピュータが行う計算方法で
and（論理積）, or（論理和）, not（否定）…
などを用いた計算方法

結果 Result



約150倍以上の
高速化に成功!!