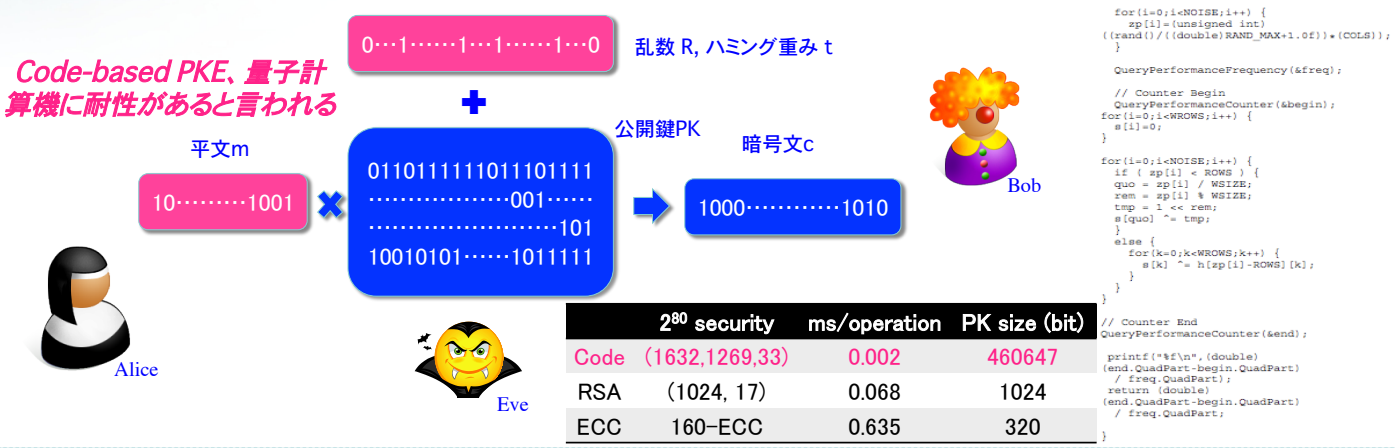
情報セキュリティ研究センター

量子計算機に耐性のある軽量公開鍵暗号/ディジタル署名方式

産総研　崔　洋(サイ　ヨウ，Cui Yang)

研究概要：現在広く普及しているRSA暗号/署名や楕円曲線暗号/署名などは、量子アルゴリズムによって効率的に解読されてしまうことが知られている。そのため、量子計算機に耐性のある**ポスト量子暗号/署名**の設計が重要な課題となっている。その際、安全性だけでなく、効率性についても実用レベルまで引き上げない限り、普及は難しい。本研究では、量子計算機に耐性を持ち、かつ、高速処理が可能なポスト量子軽量暗号/署名方式の研究を行う。



	2^{80} security	ms/operation	PK size (bit)
Code	(1632,1269,33)	0.002	460647
RSA	(1024, 17)	0.068	1024
ECC	160-ECC	0.635	320

Q.　Code-based暗号の安全性は信頼できますか？

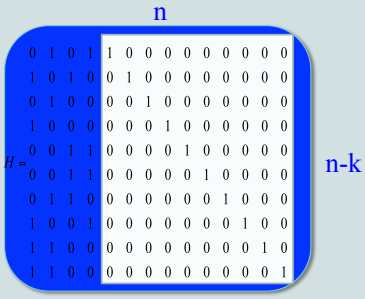
A.　暗号文cと公開鍵PKを与えられたEveが、ランダムベクトルRを知らずに平文を算出することは、NP-Hardな線形復号問題と同程度に困難と考えられている。実際に、30年以上破られていない。

既知の典型的な攻撃法：

1. Information Set Decoding Attack
2. Structural Attack
3. Syndrome Decoding Attack
4. (Generalized) Birthday Attack

本研究では、新たなセキュリティバウンドを提示。

PKを行変換で簡単化した上で、列を組み合わせて攻撃パターンを探す手法



その上で、メモリコストを効率した方式を提案：
PK(暗号の公開鍵/署名の検証鍵)のサイズは新たな技術(Flexible Quasi-Dyadic Code)で圧縮する手法を提案。(submit to AC' 10)

暗号の公開鍵/署名の検証鍵サイズ:k×(n-k)ビット(単位行列が省略)

	m	t	n	WF	検証鍵	試行回数	署名長 (bit)
従来	14	13	16384	$2^{80.7}$	360.0kb	$2^{32.5}$	182～214.5
	13	14	8192	$2^{80.0}$	178.0kb	$2^{36.4}$	182～218.4
	15	12	32768	$2^{88.2}$	86.0kb	$2^{40.3}$	180～220.3

	m	t	N	WF	検証鍵	試行回数	署名長 (bit)
提案	15	12	26528	$2^{84.0}$	48.2kb	$2^{32.5}$	180～212.5
	14	13	13316	$2^{83.4}$	22.4kb	$2^{36.4}$	182～218.4
	13	14	6736	$2^{82.9}$	10.4kb	$2^{40.3}$	182～222.3

本研究の貢献：量子計算機に耐性のある軽量公開鍵暗号方式、公開鍵が圧縮された暗号/署名方式、短い署名、鍵の匿名性、効率的に検索できる暗号、を提案した。(FY2009: DCC journal, AAECC, IEEE ICC, SCIS, submitted to IEICE, IEEE Globecom)