Cryptographic Strength of Cryptocurrency

암호 화폐의 암호학적 안전성

Mar. 7, 2018

Graduate School of Information Security
School of Computing, KAIST
IACR Fellow
Prof. Kwangjo Kim

Outline

(Abstract)

2007년 S. Nakamoto에 의거 Bitcoin이 분산 장부 기술을 암호학적 해시 함수와 타원곡선 전자서명, 계산 능력에 따른 채굴 작업을 증빙하는 소유 증명 기술 등 을 이용한 다자간 P2P 통신을 블록 체인으로 형성한 암호 화폐의 최초 탄생 후, 이더리움, 리플 등 수 천종의 암호 화폐가 전 세계에 통용되고 있다. 본 발표는 주요 암호 화폐에서 사용하는 암호 프리미티브의 암호학적 (계산량적) 안전성에 대하여 소개하고, 향후 10년 이내 상용화가 예상되는 Universal 양자 컴퓨터 공격에도 안전한 암호 화폐의 설계 필요성을 제기한다.

Keywords: Cryptocurrencies, Proof of "X", Quantum Adversaries, Post Quantum Cryptography, Quantum-resistant Cryptocurrency

Cash, E-Cash, and Cryptocurrency

	Cash	E-cash	C-Currency
Creator	Very old	D. Chaum/1982(1)	S. Nakamoto/2008(2)
Issuing Authority	National Bank	Any Bank	Entity
Trust	TTP(3)-based Centralized	TTP-based Centralized	Distributed
Network	Off-line	On-line	P2P
Security or Crypto. Tech.	Paper Printing, Watermarking	Blind Signature Crypto. Protocols Smart Card	Hash ft, Digital Signature, Block-chain, Proof-of-X Distributed ledger Smart Wallet
Double Spending	Difficult	Easy	Easy
User Privacy	High	Low	Low

(1) David Chaum,"Blind Signature for untraceable payments", Advances in Cryptology, 1982, pp. 199-203
(2) Satoshi Nakamoto, "Bitcoin : A Peer-to-Peer Electronic Cash System", 2008
TTP: Trusted-Third Party. P2P: Peer-to-Peer, B: Bank, C: Customer, S: Shop, P:Peer. ICO : Initial Coin Offering

Top 20 C-currency

No.	Name	Market Cap	BlockChain or DAG	Proof of 'X'	Mining Time
1	Bitcoin	$191,985,172,225	BC	PoW	10 min
2	Ethereum	$44,888,278,080	BC(DAG)	(PoW,) PoS	12 seconds
3	Bitcoin Cash	$26,405,485,566	BC	PoW	10 min
4	Ripple	$9,832,146,875	-	PoCons	-
5	Dash	$5,946,691,640	BC	PoW	5 seconds
6	Bitcoin Gold	$5,522,788,220	BC	PoW	2.5 min
7	Litecoin	$5,490,151,915	BC	PoW	2.5 min
8	IOTA	$5,430,535,086	DAG "Tangle"	PoW	-
9	ADA	$3,341,480,851	BC	PoS	-
10	Monero	$3,110,020,535	BC(DAG)	PoW	-
11	Ethereum Classic	$3,000,609,911	BC(DAG)	PoW	12 seconds
12	NEM	$2,571,111,000	BC	PoI	1 min
13	NEO	$2,439,229,000	BC	dBFT	20 seconds
14	EOS	$1,948,297,776	BC	DPoS	-
15	Stellar	$1,601,225,184	BC	PoCons	-
16	BitConnect	$1,012,766,466	BC	PoW, PoS	-
17	OmiseGO	$975,192,095	BC	PoS	-
18	Qtum	$974,493,915	BC	PoS	-
19	Lisk	$902,596,189	BC	DPoS	-
20	Zcash	$895,010,327	BC	PoW	2.5 min
29	Monacoin	$810,271,853	BC	PoW	1.5 min

BC: Block Chain, DAG: Directed Acyclic Graph
PoW, S, Cons, I : Proof of (Work, Stake, Consensus, Importance)
dBFT: delegated Byzantine Fault Tolerance alternative

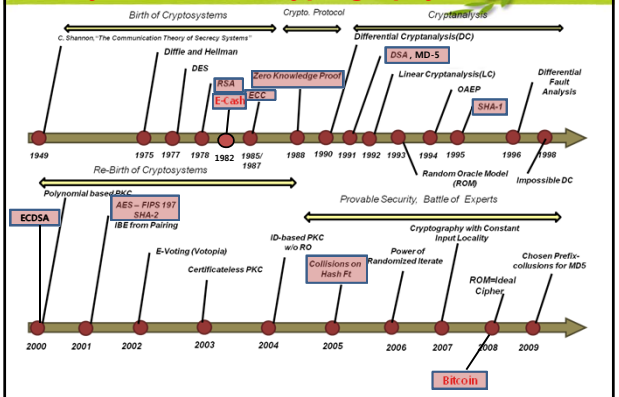
CoinmarketCap, Cryptocurrency Market Capitalizations, https://coinmarketcap.com/, accessed Dec. 4, 2017

Cryptographic primitives in Top 20 C-currency

No.	Name	Hash Algorithm	ASIC resist.	Digital Signatures	Anonymity Tech.
1	Bitcoin	SHA-256	-	ECDSA	-
2	Ethereum	Ethash	Yes	ECDSA	-
3	Bitcoin Cash	SHA-256	-	ECDSA	-
4	Ripple	80% majority	-	ECDSA	-
5	Dash	X11(SHA-3 candidates)	Yes	ECDSA	-
6	Bitcoin Gold	Equihash	Yes	ECDSA	-
7	Litecoin	Scrypt	Yes	ECDSA	-
8	IOTA	SHA-3, Kerl	-	Winternitz OTS	
9	ADA	-	-	-	-
10	Monero	CryptoNight	Yes	Ring Signature	Yes
11	Ethereum Classic	Ethash	Yes	ECDSA	-
12	NEM	SHA-256	-	ECDSA	-
13	NEO	SHA-256	-	ECDSA	-
14	EOS	SHA-3 (SHA-512)	-	ECDSA	-
15	Stellar	80% majority	-	EdDSA (Schnorr)	-
16	BitConnect	-	-	ECDSA	-
17	OmiseGO	-	-	-	-
18	Qtum	-	-	-	-
19	Lisk	-	-	EdDSA (Schnorr)	-
20	Zcash	Equihash	Yes	zk-SNARK	Yes
29	Monacoin	Lyra2RE(v2)	-	ECDSA	-

ASIC resistance : resistance against using ASIC
SHA-256 : Secure Hash Algorithm-256, SHA-3 : Secure Hash Algorithm-3, EdDSA: Ed25519 Digital Signature
ECSDA : Elliptic Curve Digital Signature Algorithm OTS: One Time Signature,
zk-SNARK : zero-knowledge Succinct Non-interactive Arguments of Knowledge

History of Modern Cryptography



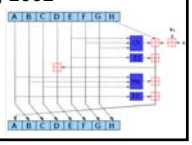
{Cryptographic} Hash Function

- Compression h(): $\{0,1\}^*$ -> $\{0,1\}^n$
  - For identification, integrity, hash-and-sign
- One-wayness
  - Pre-image resistance: Given *y*, it is computationally infeasible to compute *x* with *y=h(x)* -> *Pre-image Attack*
  - Second pre-image resistance: Given *x* and *h(x)*, it is computationally infeasible to compute *x'* with *h(x)=h(x')*
- Collision-free (Prevent internal misuse)
  : It is computational infeasible to find a pair *(x, x')*, $x \neq x'$ satisfying *h(x)=h(x')*. -> *Birthday Attack*
- Efficiency
  - Easy to compute *h(x)* for a given *x*.

Dedicated Hash Function

- MDx family: proposed by Rivest
  - MD4, Crypto'90
  - MD5, RFC 1992

- SHA family: proposed by NIST
  - SHA-0, FIPS-180, 1993
  - SHA-1, FIPS-180-1, 1995
  - SHA-2 (SHA-256/384/512), FIPS-180-2, 2002



Real & Fake Certificate using MD-5 with RSA

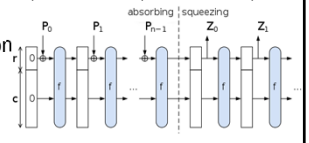
This page is intentionally blank.

SHA-3 (1/2)

- Drop-in replacement of SHA-2
- Collision resistance of approximately *n/2* bits ($2^{n/2}$ computations)
- Pre-image resistance of approximately *n* bits
- Second-preimage resistance of approximately *n-k* bits for any message shorter than 2^k *bits* (for MD construction)
- Resistance to length-extension attacks
- Eliminate length-extension property
- Tunable security/performance tradeoff

SHA-3 (2/2)

- Keccak Designed by G. Bertoni, J. Daemen, M. Peeters, G. Van Assche / 2015
- Flexible Sponge Construction



- Instances

Instance	Output size *d*	rate *r* = block size	capacity *c*	Definition	Security Strengths in Bits		
					Collision	Preimage	2nd Preimage
SHA3-224(*M*)	224	1152	448	Keccak[448](*M* ‖ 01, 224)	112	224	224
SHA3-256(*M*)	256	1088	512	Keccak[512](*M* ‖ 01, 256)	128	256	256
SHA3-384(*M*)	384	832	768	Keccak[768](*M* ‖ 01, 384)	192	384	384
SHA3-512(*M*)	512	576	1024	Keccak[1024](*M* ‖ 01, 512)	256	512	512
SHAKE128(*M*, *d*)	*d*	1344	256	Keccak[256](*M* ‖ 1111, *d*)	min(*d*/2,128)	≥min(*d*,128)	min(*d*,128)
SHAKE256(*M*, *d*)	*d*	1088	512	Keccak[512](*M* ‖ 1111, *d*)	min(*d*/2,256)	≥min(*d*,256)	min(*d*,256)

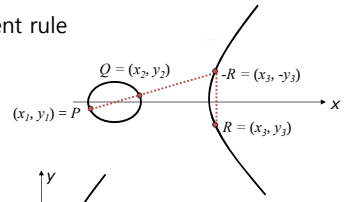
Comparison of SHA functions

Algorithm and variant	Output size (bits)	Internal state size (bits)	Block size (bits)	Max message size (bits)	Rounds	Operations	Security bits (bits)	Capacity against length extension attacks	Performance on Skylake (median cpb) long messages	Performance on Skylake (median cpb) 8 bytes	First Published
MD5 (as reference)	128	128 (4 × 32)	512	Unlimited	64	And, Xor, Rot, Add (mod 2^{32}), Or	<64 (collisions found)	0	4.99	55.00	1992
SHA-0	160	160 (5 × 32)	512	$2^{64}-1$	80	And, Xor, Rot, Add (mod 2^{32}), Or	<34 (collisions found)	0	≈ SHA-1	≈ SHA-1	1993
SHA-1							<63 (collisions found)		3.47	52.00	1995
SHA-2 SHA-224	224	256 (8 × 32)	512	$2^{64}-1$	64	And, Xor, Rot, Add (mod 2^{32}), Or, Shr	112	32	7.62	84.50	2004
SHA-256	256						128	0	7.63	85.25	2001
SHA-384	384	512 (8 × 64)	1024	$2^{128}-1$	80	And, Xor, Rot, Add (mod 2^{64}), Or, Shr	192	128 (± 384)	5.12	135.75	
SHA-512	512						256	0	5.06	135.50	
SHA-512/224	224						112	288	≈ SHA-384	≈ SHA-384	
SHA-512/256	256						128	256			
SHA-3 SHA3-224	224	1600 (5 × 5 × 64)	1152	Unlimited	24	And, Xor, Rot, Not	112	448	8.12	154.25	2015
SHA3-256	256		1088				128	512	8.59	155.50	
SHA3-384	384		832				192	768	11.06	164.00	
SHA3-512	512		576				256	1024	15.88	164.00	
SHAKE128	*d* (arbitrary)		1344				min(*d*/2, 128)	256	7.08	155.25	
SHAKE256	*d* (arbitrary)		1088				min(*d*/2, 256)	512	8.59	155.50	

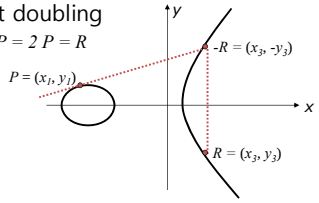
Bitcoin Developed in 2008

Elliptic Curve

- Chord-and-tangent rule
  $P + Q = R,\ P \neq Q$



- Point doubling
  $P + P = 2P = R$



ECDSA*

Alice	Bob
Parameters $D = (q, a, b, G, n, h)$ Associated keys (d, Q)	Parameters $D = (q, a, b, G, n, h)$ Alice's public key Q Alice's signature (r, s) on m
To sign message m: 1. k randomly chosen $0 < k < n-1$ 2. $k \cdot G = (x_1, y_1)$ $r = x_1 \bmod n$ 3. if $r = 0$ abort and start again 4. e = SHA-1(m) 5. $s = k^{-1} \cdot (e + d \cdot r) \bmod n$ 6. if $s = 0$ abort and start again **Output:** (r, s)	**To verify signature (r, s):** 1. check: $1 \le r \le n-1,\ 1 \le s \le n-1$ 2. e = SHA-1(m) 3. $w = s^{-1} \bmod n$ 4. $u_1 = e \cdot w \bmod n$ $u_2 = r \cdot w \bmod n$ 5. $X = u_1 \cdot G + u_2 \cdot Q$, if $X = O \rightarrow$ reject 6. $X = (x_1, y_1)$ $v = x_1 \bmod n$ 7. if $v = r \rightarrow$ accept

D, Q, m, r, s

Proof that signature verification works:

$$s = k^{-1}(e + dr) \bmod n \Leftrightarrow k \equiv s^{-1}(e + dr) \equiv s^{-1}e + s^{-1}rd \equiv we + wrd \equiv u_1 + u_2 d \bmod n$$

$$u_1 G + u_2 Q = (u_1 + u_2 d)G = kG \quad \Rightarrow \quad v = r$$

* : NIST FIPS 186-4, Jul. 2016

RSA Public-key Cryptosystem

1. $(pk_B, sk_B) \leftarrow \text{KeyGen}(1^\lambda)$
   - Choose two distinct prime numbers p and q.
   - Compute $N = pq$ and $\phi(N) = (p-1)(q-1)$ where $\phi(x)$ is Euler's totient function.
   - Choose an integer e s.t. $1 < e < \phi(N)$ and $\gcd(e, \phi(N)) = 1$.
   - Determine d s.t. $ed \equiv 1 \pmod{\phi(N)}$.
2. Key distribution
   - Bob sends public key $pk_B = (N, e)$ to Alice and keeps secret key $sk_B = (d)$.
3. $c \leftarrow \text{Enc}_{pk_B}(m)$
   - Alice encrypts m and sends $c \equiv m^e \pmod N$ to Bob.
4. $m \leftarrow \text{Dec}_{sk_B}(c)$
   - Bob receives c and decrypts $m \equiv c^d \pmod N$.
   - Using Euler's theorem $a^{\phi(N)} \equiv 1 \pmod N$ if $\gcd(a, N) = 1$:
     $c^d = m^{ed} = m^{1+h\phi(N)} = m \pmod N$

Breaking PKC by Classical & Quantum Computers

For each RSA number N, there exist prime numbers p and q s.t. $N = pq$.
The problem is to find these two primes given only N!

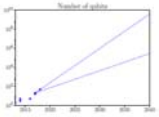
Classical computer	Quantum computer
• The general number field sieve is the most efficient classical algorithm known for factoring integers larger than 10^{100}.	• Shor's algorithm is a quantum algorithm for integer factorisation.
• takes sub-exponential time about $O\left(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}}\right)$	• would be able to take polynomial time about $O\left((\log N)^2(\log\log N)(\log\log\log N)\right)$
• The largest factored RSA number is 768 bits long while the typical key size is 1024 to 4096 bits long. It takes around 1500 CPU years (2 years of real time with hundreds of computers)	• The largest factored RSA number is 21 using Shor's algorithm

(Note) DLP and EC-DLP are same intractable problems like IF in RSA.

Quantum Computer

Year	# of qubits
2013	2
2014	5
2014	3
2016	5
2017	16
2017	20
2018	49

(1)



- Quantum mechanics applies to all systems from micro to macro scale and enables superposition and entanglement.
- Reversible computing: if no information is erased, computation may in principle be achieved which is thermodynamically reversible, and require no release of heat

(1) D. Aggarwal et al. "Quantum attacks on Bitcoin, and how to protect against them", arXiv 1710.10377v1. Oct. 28, 2017

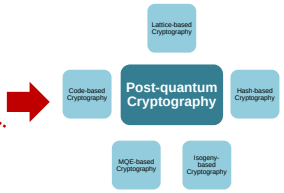
Post Quantum Cryptography (1/2)

Number-Theoretic PKC

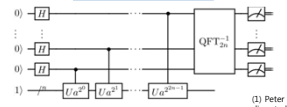
- Integer Factorization
- Discrete-Logarithm
- Elliptic-Curve DL

RSA

DH



Shor Algorithm(1)



(1) Peter W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM Journal on computing 26.5 (1997): 1484-1509

Post Quantum Cryptography (2/2)

Revisiting the NSA Suite B Annoucement

- '15.8: "양자 내성을 가지는 암호 Suite로 전환할 계획" 발표
  - 기존의 암호 Suite B를 폐기
- https://www.nsa.gov/what-we-do/information-assurance/

NIST PQC Call-for-proposal

- '16.12: "양자컴퓨터 공격에 안전한 각종 암호 프리미티브 공모" 계획 발표
- '17.11: PQC Call-for proposal
- https://www.nist.gov/pqcrypto

Experiment by Google Canary

- '16.7: 양자컴퓨터의 상용화에 대비하여 NewHope(1) 프로토콜 추가
  - 래티스 기반 PQC 기술이 내장된 세계 최초의 상용 서비스 시도
- https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html

(1) E. Alkim, *et al* "Post-quantum Key Exchange – a new hope." Cryptology ePrint Archive, Report 2015/1092, 2015.

Concluding Remarks

- Useless broken ciphers
  - DES : 2^{56}('77) -> 2^{47}('92)
  - RSA : RSA-330 ('91) -> RSA-768(2010)
  - MD-5 : '91 ->2004
- Moore's law -> Quantum Moore's law
  - Universal quantum computer will appear in 10 years
  - ECDSA will be cracked in 30 min using 485,550 qubits(1)
- Quantum-safe c-currency like QRL(2) guarantees for long time security
- No security proof in most C-currency except ouroboros(3)
- (For Students) Attend CS448 and CS548 for details

(1) D. Aggarwal et al. "Quantum attacks on Bitcoin, and how to protect against them", arXiv 1710:10377v1. Oct. 28, 2017
(2) Quantum Resistant Ledger, peterwaterland@gmail.com. Nov. 2016
(3) Aggelos Kiayias, Alexander Russell, et al, "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol", Aug. 21, 2017

Q&A

THANK YOU!