전자화폐의 분류

- 신용카드 형
  - Network 형 : PC에 내장된 전용 S/W에 카드 정보를 기억시키고 암호화된 카드 정보는 중계 시스템의 중재로 결재에 이용 (Cyber Cash, Smart Wallets)
  - 사전 등록형 : 일종의 회원 등록 형태로 카드 정보를 사전 등록하고 전용회원 번호로 네트워크에 결재, 전자우편을 이용 확인, 취소(First Virtual)
- 화폐형
  - Network 형 : 네트워크 상에 가상의 coin을 생성, 결재에 이용 (e-Cash)
  - Card 형 : IC 카드 상에 현금 가치를 이전하는 잔고 보증 가능한 선불형 전자 지갑, 양도 가능 (Mondex)
- 전자 수표
  - IC 카드에 내장된 전자수표장과 전자 서명을 이용한 네트워크 상의 수표(FSTC:Financial Services Technology Consortium)

© 한국정보통신대학원 김 광조

가치 이전 여부에 의한 분류

- 잔고관리형
  - 공통키 형 : 본인확인 및 데이터 송수신에 비밀 키 암호 사용
  - 공통키 형(정적인증있음) : 데이터송수신에 비밀키암호를 이용하나 본인이 소지하고 있는 카드의 인증은 센터의 비밀키에 의해 서명한 증명서에 의한 방식
  - 공개키 형(동적인증있음): 본인확인을 공개키암호를 이용한 동적인증(지불시에는 Challenge(상점명,금액,시각 등)에 대한 서명을 생성)에 의한 방식. 데이터 송수신에 암호를 이용가능

© 한국정보통신대학원 김 광조

가치 이전 여부에 의한 분류(계속)

- 전자증서형
  - 공통키 형 : 본인 확인 및 데이터 송수신에 비밀키를 사용하고 발행기관이 할당한 비밀번호등을 포함한 전자증서(서명없음)를 송신하는 것에 의해 가치를 이전하는 방식
  - 공개키 형(정적인증있음) : 본인확인을 센터의 비밀키에 의해 서명된 증명서에 위한 방식. 단, 전자서명서 자체는 센터의 비밀키에 의해 서명
  - 공개키 형(동적증명있음) : 본인확인을 공개키 암호를 이용하여 동적인증(지불시에는 Challenge{상점명, 금액, 시각 등}에 대한 서명을 생성)

© 한국정보통신대학원 김 광조

전자화폐의 분류(계속)

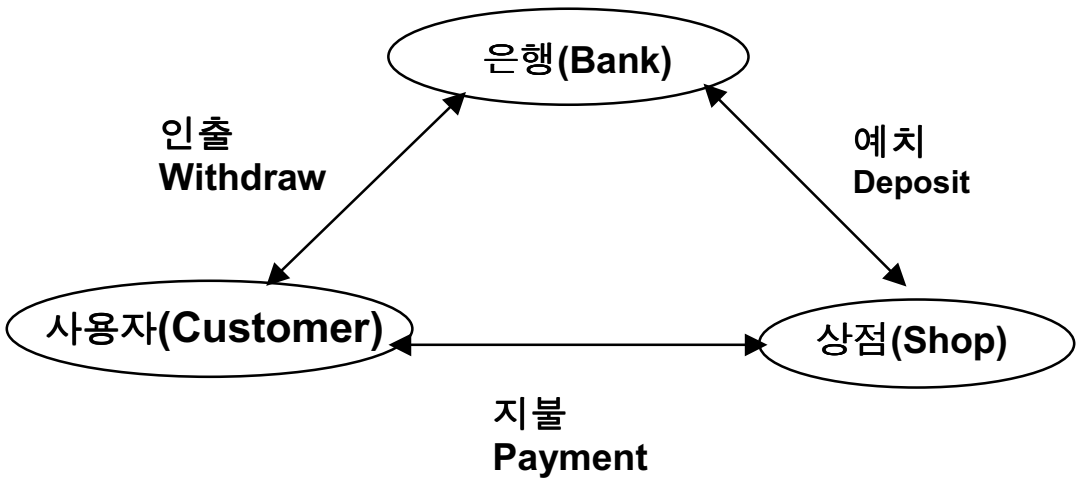
가치관리방식	잔고관리형										전자증서형			
유통형식	closed-loop						open-loop				closed-loop		open-loop	
가치관리장소	local		병용		센터		local		센터		local (전자증서형의 특징)			
센터 접속	off	on	off	on	off	on	off	on	off	on	off (사후)	on (즉시)	off (사후)	on (즉시)
모델 유무	O	X(1)	O	X(1)	X(2)	O	O	X(3)	X(2)	X(3)	O	X	O	X(3)

(1) 센터에 on-line 접속 시 local에 가치 보존은 무의미
(2) 센터에 on-line 접속하지 않고 센터에서 잔고를 관리하는 것은 무의미
(3) open-loop형은 "이용자에서 이용자로 센터의 개입없이 자치를 전달 가능"한 것을 의미함. 이런 의미에서 거래 시 센터에 접속하는 정보의 취급은 open-loop라고 하지 않음.

© 한국정보통신대학원 김 광조

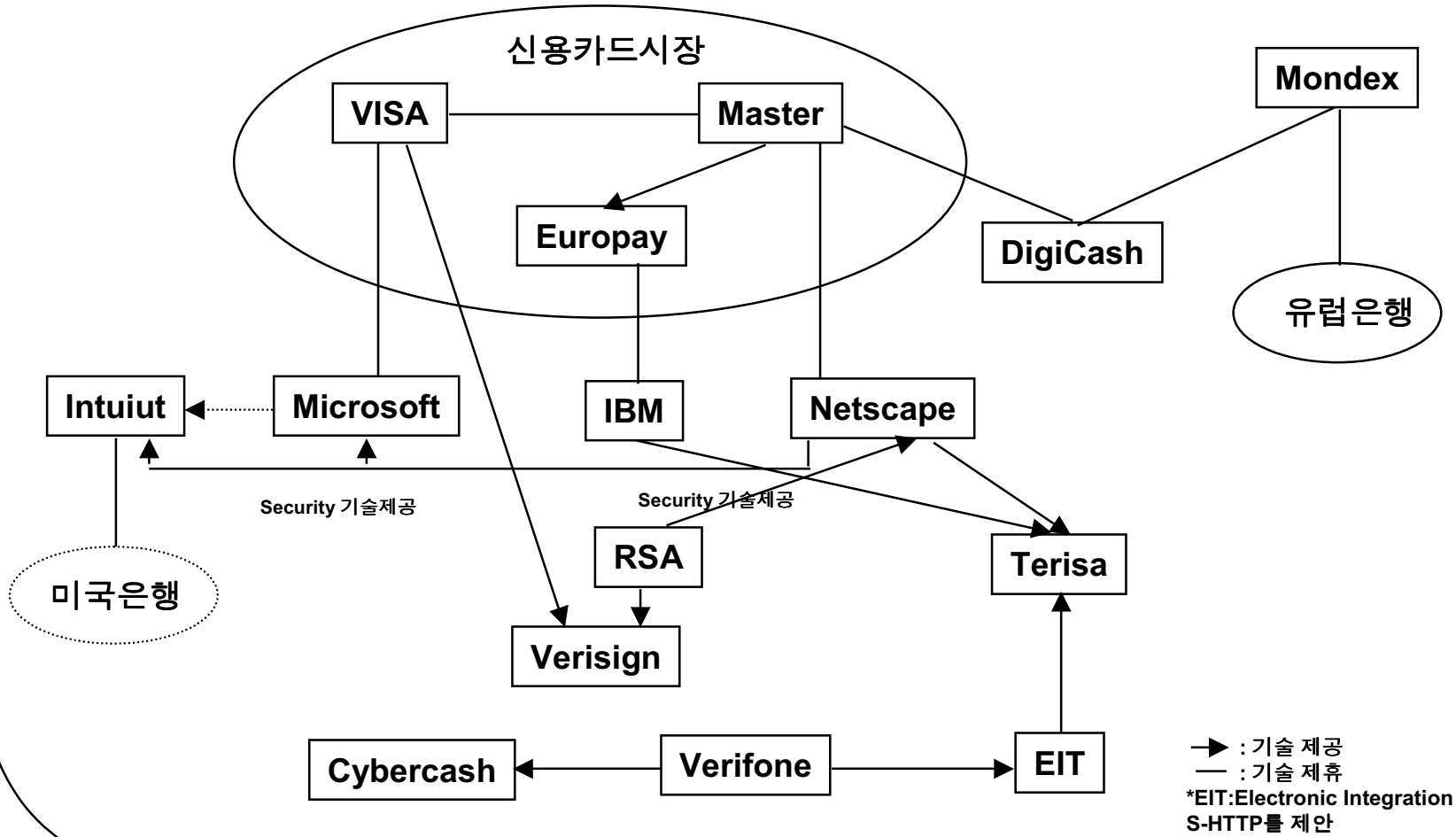
전자 결제의 기본 프로토콜

- 소비자가 은행에서 예금 인출
- 소비자가 상점으로 지불
- 상점에서 은행으로 예치



© 한국정보통신대학원 김 광조

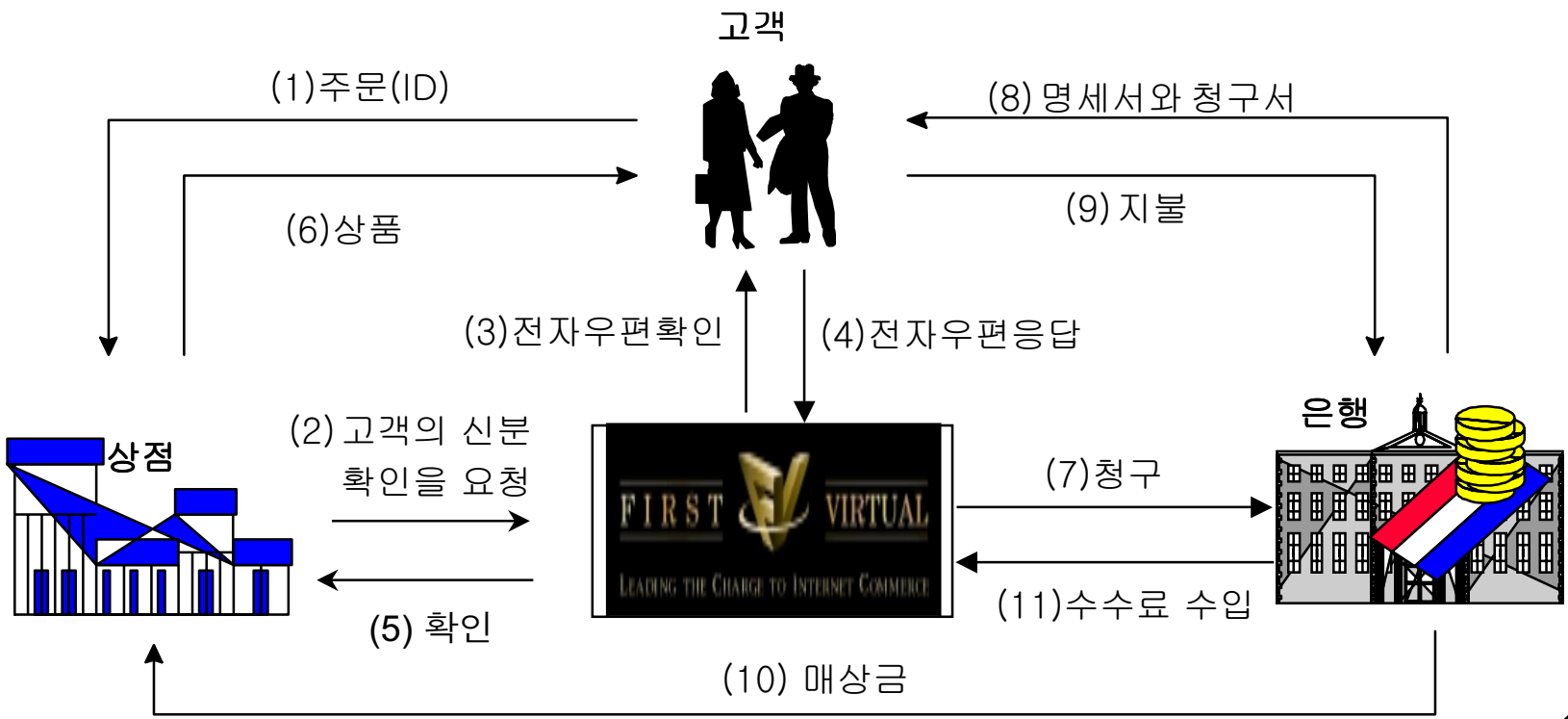
전자지불 서비스 회사간 관련도



© 한국정보통신대학원 김 광조

First Virtual

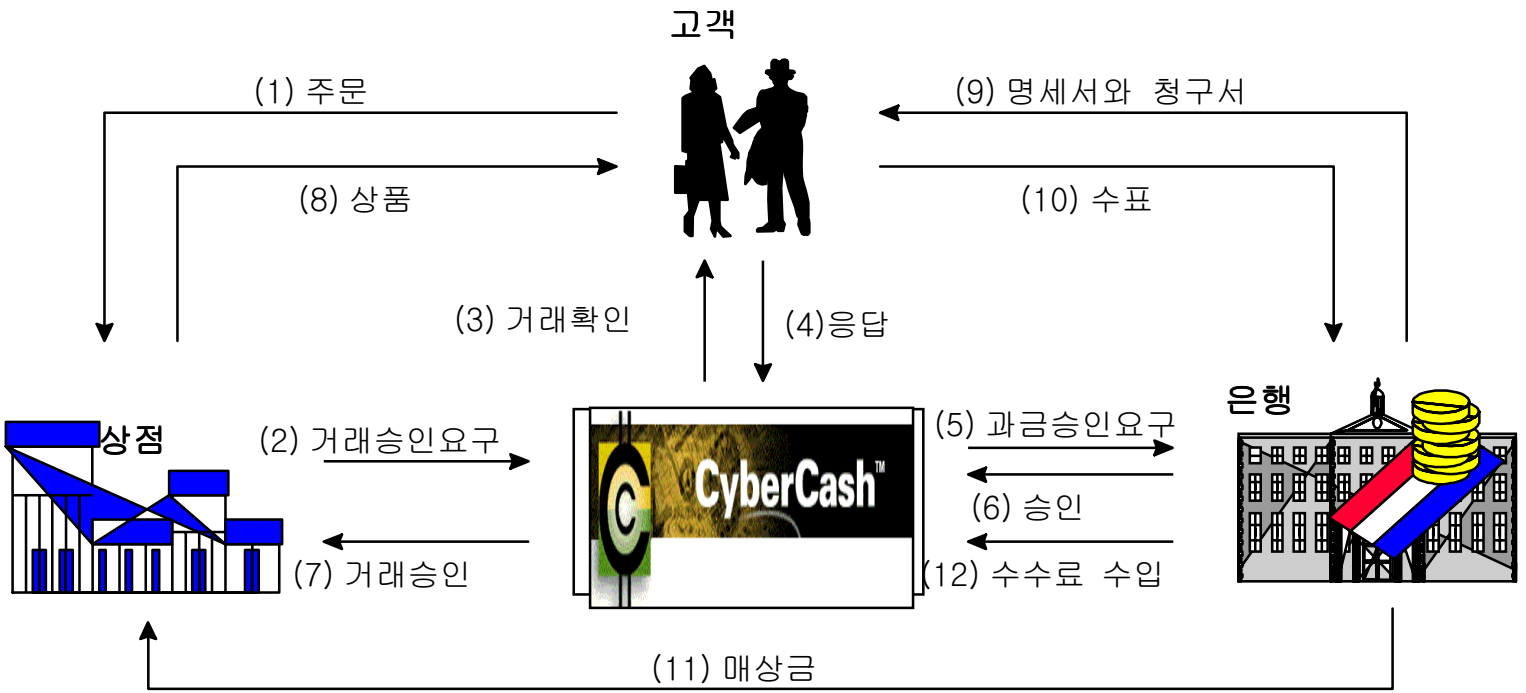
- 개인의 신상정보를 전화등을 이용해 등록해 두고 ID 번호를 이용자에게 발행하는 방식, 전자 우편을 이용
- 암호 기법을 사용하지 않음 (http://www.fv.com)



© 한국정보통신대학원 김 광조

Cyber Cash

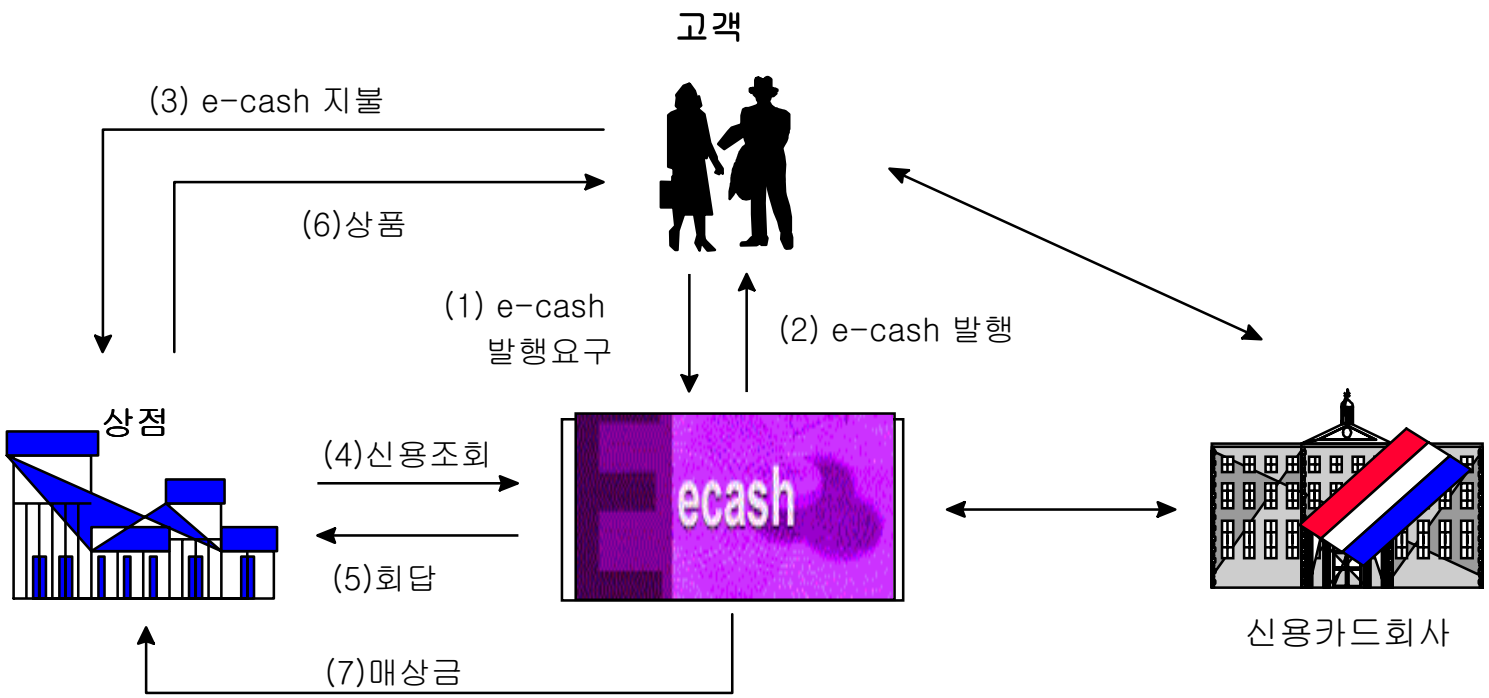
- 전용 소프트웨어를 사용 (http://www.cybercash.com)
- 사용자의 신용카드 정보는 786비트 RSA 암호화되어 전송됨



© 한국정보통신대학원 김 광조

e-Cash

- DigiCash (http://www.digicash.com)사에서 개발
- 전자화폐 개념에 기반



Mondex

- 영국의 몬덱스사 (http://www.mondex.com)에서 개발
- 스마트 카드를 이용한 오프라인 방식

© 한국정보통신대학원 김 광조

기존 전자화폐의 유형별 기능

종류/ 구분	범용선불형 전자화폐	Off-line 직불형 전자화폐	Mondex형 전자화폐
화폐저장 기능	O	O	O
저장시 비밀번호 사용	O	O	O
거래전 이자 지급	X	O	X
거래시 비밀 번호 사용	X	O	X
예금 인출 시점	저장시	통보시	저장시
단말기 방식	Off-line	Off-line	Off-line
은행간 차액 결재	O	O	X
카드 간 자금 이체	X	X	O
법정 화폐성	X	X	O

© 한국정보통신대학원 김 광조

지불방식의 비교

평가항목 / 조건명	구분 / 개 요	기존서비스		기존전자결재/현금방식			이상형 전자 화폐 방식
		현금	신용카드	인터넷 신용카드이용	IC 카드 온라인 체크	IC 카드 물리적인 기구	
완전정보화	Bit 만이 기본 요소	X	X	O	O	X	O
재사용불가능	복사에 의한 부정 이용을 할 수 없음	U	U	U	O	U	O
프라이버시	이용자의 구매이력이 노출되지 않음	O	X	O/X	X	O	O
오프라인성	은행이 개입하지 않음	O	X	X	X	O	O
양도 가능성	개인간 양도가능	O	-	U	U	O	O
분할이용 가능성	액면 금액만큼 분할이용 가능	X	-	-	X	O	O

O : 조건 만족, X : 조건 불만족, U : 제약 조건, - : 의미 없음

© 한국정보통신대학원 김 광조

현재 사용되는 전자지불시스템 현황

유형		제품	안전성	불추적성	이중사용 방지	오프라인	양도성	분할성	n회사용 가능
네트워크형	전자화폐	Ecash	o	o	o	온라인	x	x	x
	신용 카드 기반	FV	o	x	-	온라인	x	x	x
		Cyber Cash	o	x	-	온라인	x	x	x
	전자 수표 기반	NetCheque	o	x	o	온라인	x	x	x
		Echeck	o	x	o	온라인	x	x	x
전자지갑형	영국	Mondex	o	o	o	오프라인	o	x	x
	벨지움	Proton	o	o	o	오프라인	x	x	x
	포르투칼	MEP	o	o	o	오프라인	x	x	x
	덴마크	Danmont	o	o	o	오프라인	x	x	x
	핀란드	AVANT	o	o	o	오프라인	x	x	x
	독일	Chipknip	o	o	o	오프라인	x	x	x
	한국형	전자지갑	o	x	o	오프라인	x	x	x

© 한국정보통신대학원 김 광조

종이화폐와 전자화폐의 비교

종이 화폐	전자 화폐	
-유통성 →	- 완전 정보화 (complete information)	기본조건
	- 오프라인성(Off-line)	
	- 양도성(Transivity)	
-상징성(유일성) →	- 안전성 (Security)	
	- 불추적성(Untraceability)	
-익명성(프라이버시) →	- 재(이중)사용 불가능성(Unreusability)	
	- n회 사용 가능	추가조건
	- 분할성(Divisability)	

© 한국정보통신대학원 김 광조

종이화폐의 완전 불 익명성

- 부피 : 많은 돈은 부피를 차지
- 처리 지연 : 전달 및 확인 시간 소요
- 감지 가능성(Palpability) : 실제 현금은 전산망으로 전달될 수 없고 멀리 있는 수신자에게 안전하게 전달하기 위해 시간 소요
- 추적 가능성 : 화폐의 일련번호로 추적 가능

© 한국정보통신대학원 김 광조

익명성 제어

(1) 합법적인 사용자를 위한 익명성

(2) 명령서에 의한 취소 (Revocation upon warrant presentation)

(3) 권한의 분산 (Separation of power)

(4) 모방 불가 (No framing)

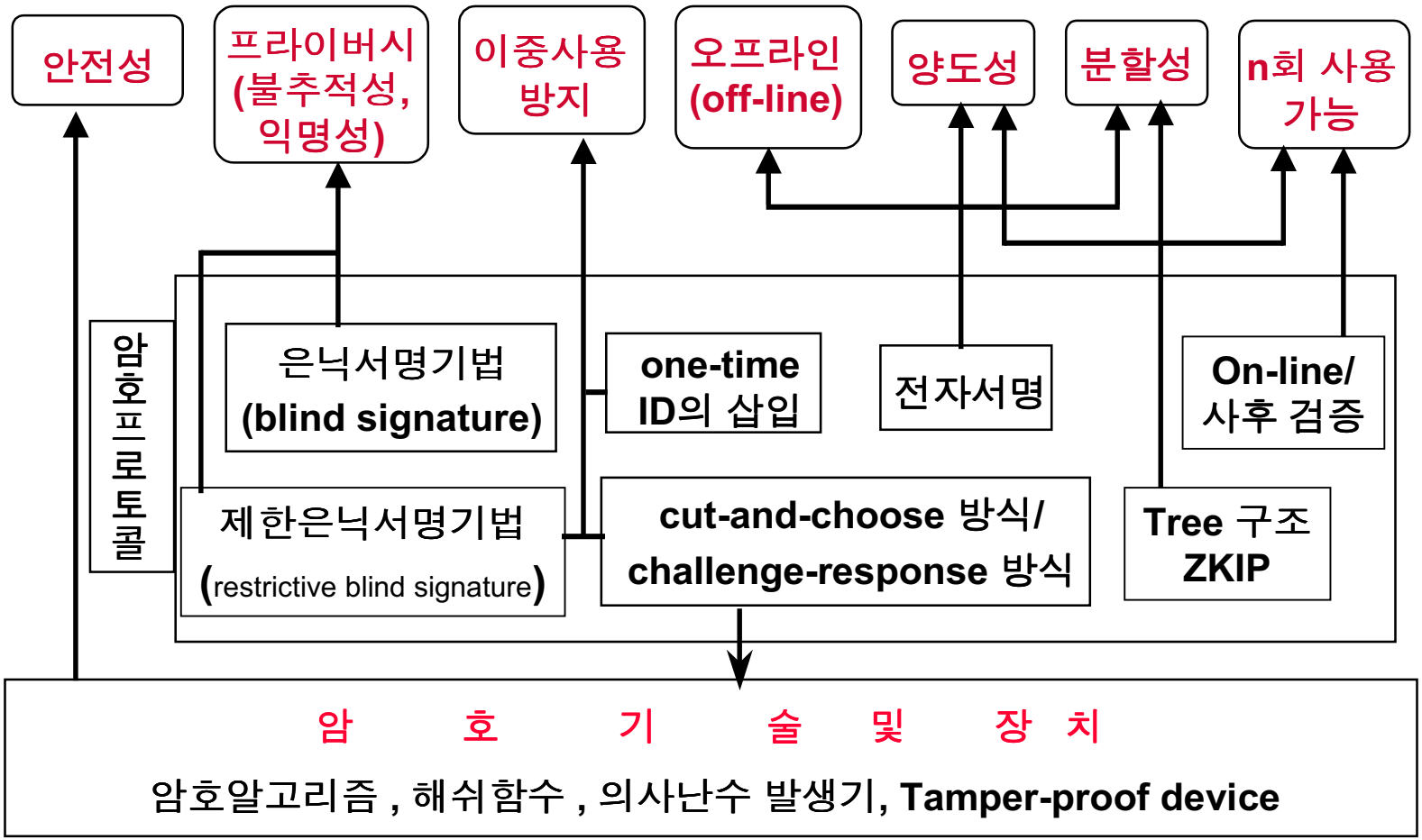
(5) 선택성 (Selectivity)

(6) 효율성 (Efficiency)

(7) 범죄 방지 (Crime prevention)

© 한국정보통신대학원 김 광조

전자화폐와 암호 기술



© 한국정보통신대학원 김 광조

이중사용 방지 대책

- 복제할 수 없는 장치 사용
- 전자화폐 발행 시 온라인 검증
- 지불 후 부정을 검출할 수 있는 구조를 강구 (오프라인 검증)
  - Claw-free 함수 이용
  - ZKP이용 방식
  - 소인수 분해 이용 방식
  - 이산 대수 문제 방식

© 한국정보통신대학원 김 광조

전자 화폐의 연구 역사

81년 : Chaum의 untraceabilty 연구

82년 : Chaum의 on-line, 추적불가능한 전자화폐를 위한 blind signature 연구

83년 : Even 등의 off-line 방식으로 RSA암호와 Tamper proof device를 이용한 전자 지갑 제안

85년

- Chaum등에 의한 추적불가능한 blind 서명 연구
- On-line 전자 화폐를 Damgard가 제안

88년

- *D.Chaum 등에 의해 최초로 이론적인 전자화폐 방식[CFN88]인 추적불가능한 전자화폐 제안
- On-line 전자 화폐를 Damgard가 제안

전자 화폐의 연구 연사(계속)

89년

- On-line 전자 화폐를 Chaum도 제안
- Okamoto와 Ohta가 ZKIP와 추적 불가능성을 연계한 transferability를 제공하는 전자화폐 방식 제안
- CFN88방식의 효율을 개선한 방식을 Chaum 제안

90년 :

- Heyes가 1회용 추적 불가능 서명을 이용 전자화폐 제안
- CFN88 방식을 개선한 효율적인 off-line 전자화폐를 Antwerpen이 제안

91년 :

- Okamoto와 Ohta의 분할 가능한 전자화폐[OO91]
- Damgard가 on-line 전자화폐의 추적 가능성을 지적하고 개선안 제안
- Antwerpen의 방식의 문제점을 지적 개선 방안을 Hirschfeld가 제안

출처 : 박춘식,이대기,“전자화폐가 세계를 바꾼다”,한국통신정보보호학회지 제6권,제2호, 1996.6.

© 한국정보통신대학원 김 광조

전자 화폐의 연구 연사(계속)

92년

- Tamper-proof device를 이용한 전자 지갑 제안
- Transferable 전자화폐는 정보량 증가 없이는 구현 불가능성을 Chaum 과 Pederson이 증명
- Schnorr 방식을 이용, 분할 가능한 전자화폐 제안

93년

-*Brands, Ferguson, Yung 등이 효율적인 Challenge/Response 방식의 전자 화폐[Brands93] 제안
- 기존 전자지갑의 Privacy를 개량한 방식 제안 (Cramer, Pederson)
- 지불단계에서 Schnorr의 인증 방식을 이용한 전자화폐 방식과 필요시 추적 가능한 전자화폐방식 제안

© 한국정보통신대학원 김 광조

전자 화폐의 연구 역사(계속)

94년

- S. Brands의 전자 화폐를 분할성을 증가한 방식 제안
- ElGamal 서명 방식을 이용한 전자화폐를 제안하여 Brands의 효율성 개선

- NIZK에 안전성을 둔 추적 불가능성 전자화폐를 D'Amiano와 Crescenzo가 제안하고 Transferable 하더라고 정보량 증가 않는 방식 제안

95년

-NIZK를 이용한 전자화폐가 추적 가능함을 Pfitzmann등이 보임

-전자화폐에서의 추적 불가능성이 돈 세탁등의 범죄에 악용될 수 있는 문제를 해결하고자 공정한 내용은닉 서명을 제안

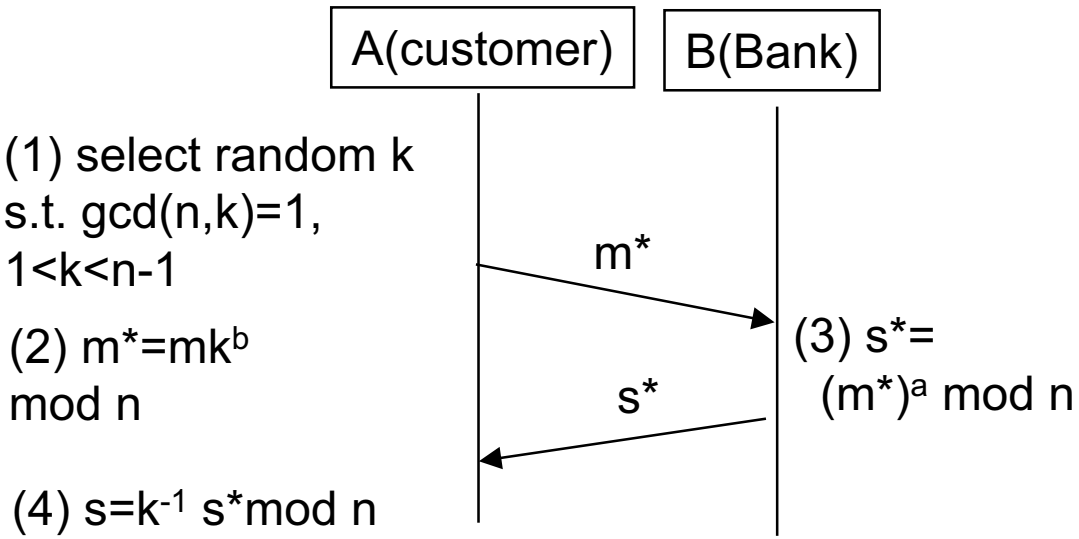
-전자화폐의 지불단계에서의 구매자와 상점간의 공정한 거래를 제공방안

-내용은닉 서명보다 Secret-key certificate개념을 도입 효율적인 전자화폐 방안 제안

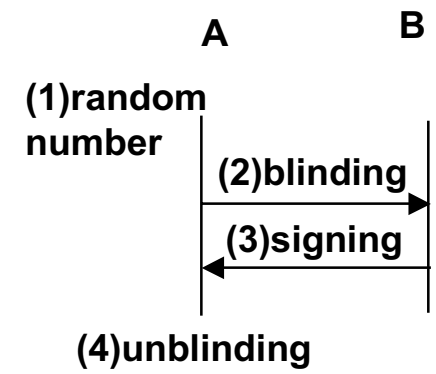
© 한국정보통신대학원 김 광조

Chaum's Blind Signature

- A가 B에게 메시지의 내용을 모르게 하면서 서명을 받는 방식으로 A의 익명성 보장에 이용
- B의 RSA 암호용 공개키 :{n,b}, 비밀키:{a}



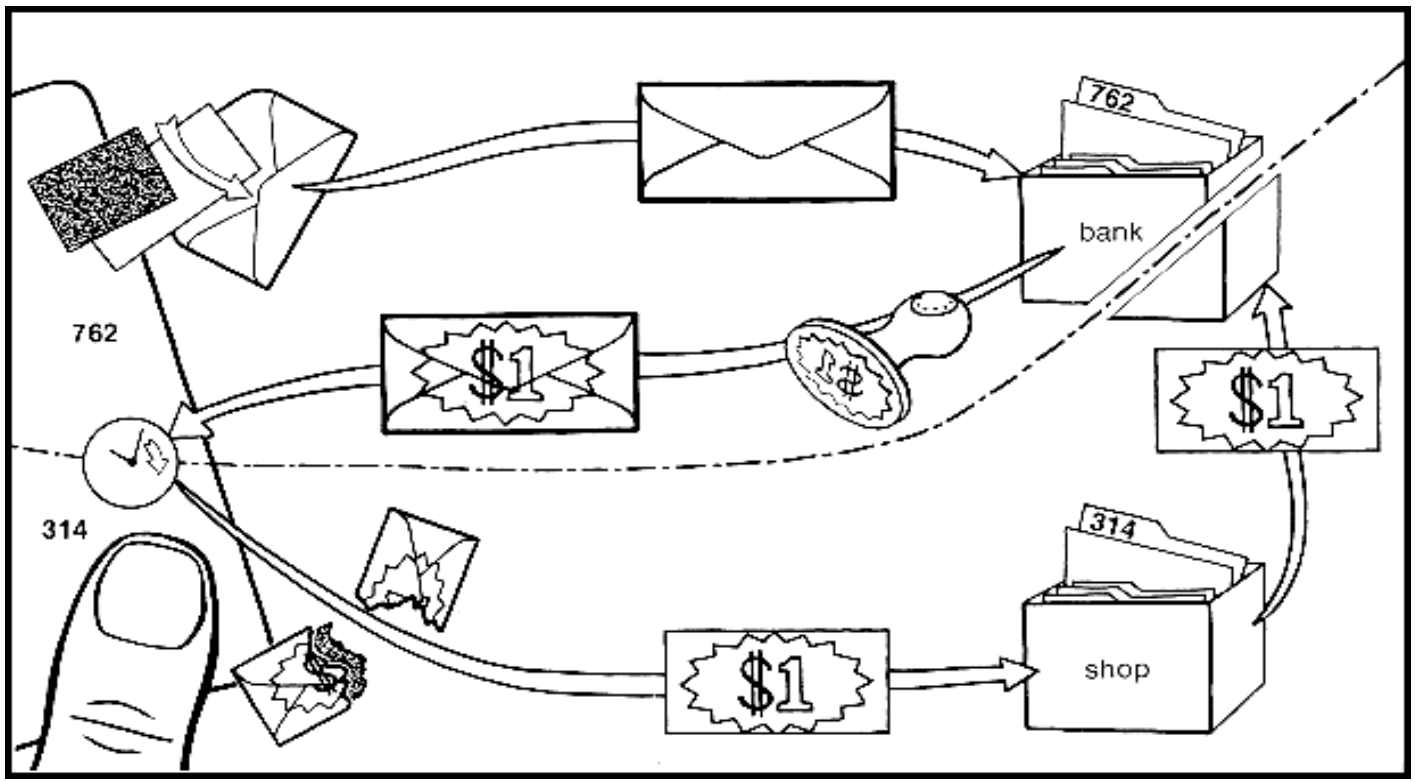
(B의 M에 대한 서명 $k^{-1}(mk^b)^a = k^{-1} m^a k^{ba} = m^a$)



$g(S_B f(m)) = S_B(m)$
f:blinding ft
g:unblinding ft only A knows
f(m) : blinded message

Chaum's Blind Signature(예)

묵지를 이용한 내용 은닉 서명



© 한국정보통신대학원 김 광조

Chaum's Blind Signature(예)

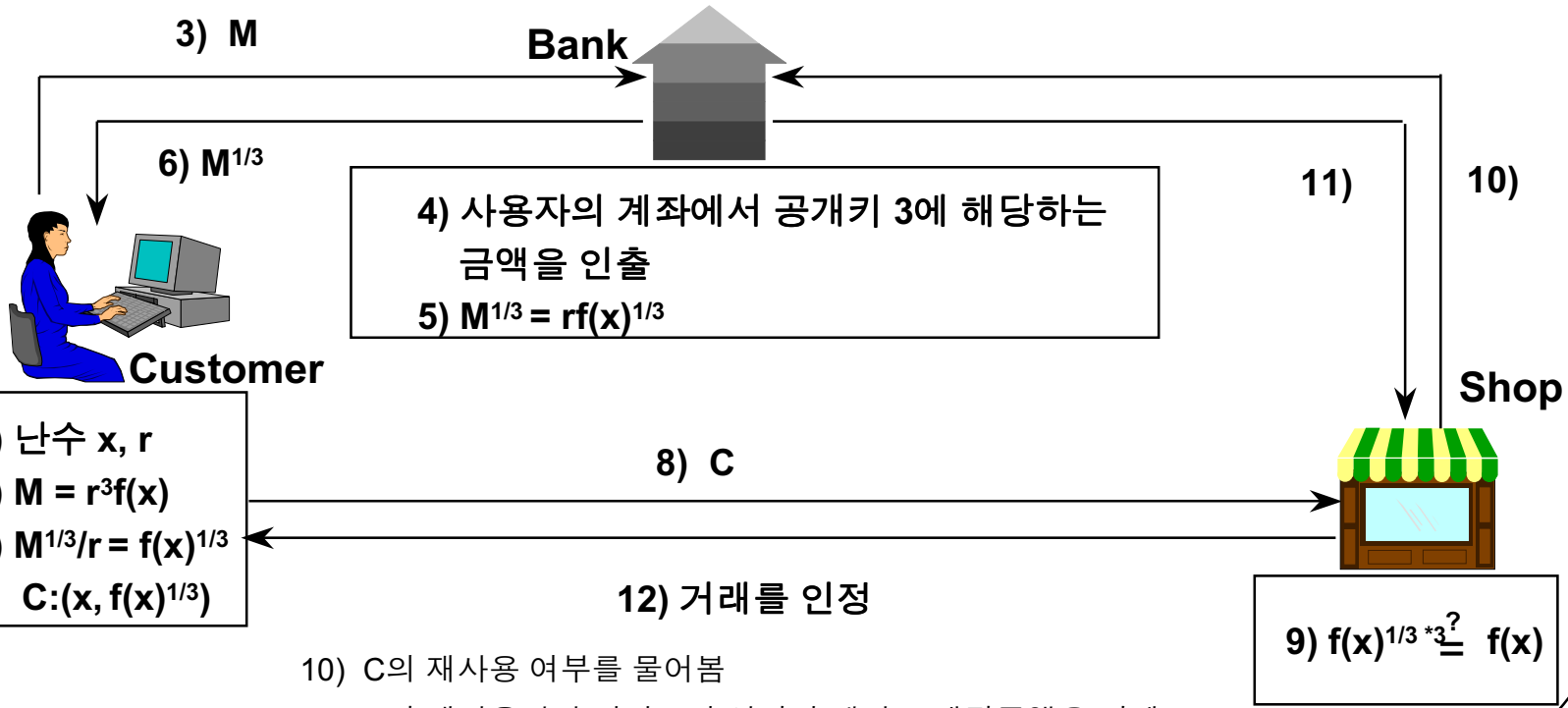
(준비) p=11, q=3, n=33,ϕ(n)= 10 * 2=20
gcd(a, ϕ(n))=1 => a=3, ab =1 mod ϕ(n) => 3 b = 1 mod 20 => b=7
B의 public key :{n,b}={33,7}, secret key ={a}={3}

(1) A의 blinding of m=5
select k s.t. gcd(k,n)=1 => gcd(k,33)=1 => k=2
$m^* = m\ k^b \bmod n = 5\ 2^7 \bmod 33 = 640 = 13 \bmod 33$
(2) B's signing
$s^* = (m^*)^a \bmod n = 13^3 \bmod 33 = 2197 = 19 \bmod 33$
(3) A's unblinding
$s = k^{-1}\ s^* \bmod n$ ($2\ k^{-1} = 1 \bmod 33 \Rightarrow k = 17$)
$= 17\ 19 \bmod 33 = 323 = 26 \bmod 33$
(*)원래의 서명문 : $m^a \bmod n = 5^3 \bmod 33 = 125 = 26 \bmod 33$

© 한국정보통신대학원 김 광조

RSA 암호를 이용한 온라인형 전자화폐

- f : 해쉬함수
- n : n=p*q의 합성수 p,q는 은행만이 알고 있음
- 3,1/3 : 일정한 금액에 해당하는 은행의 공개키 및 비밀키

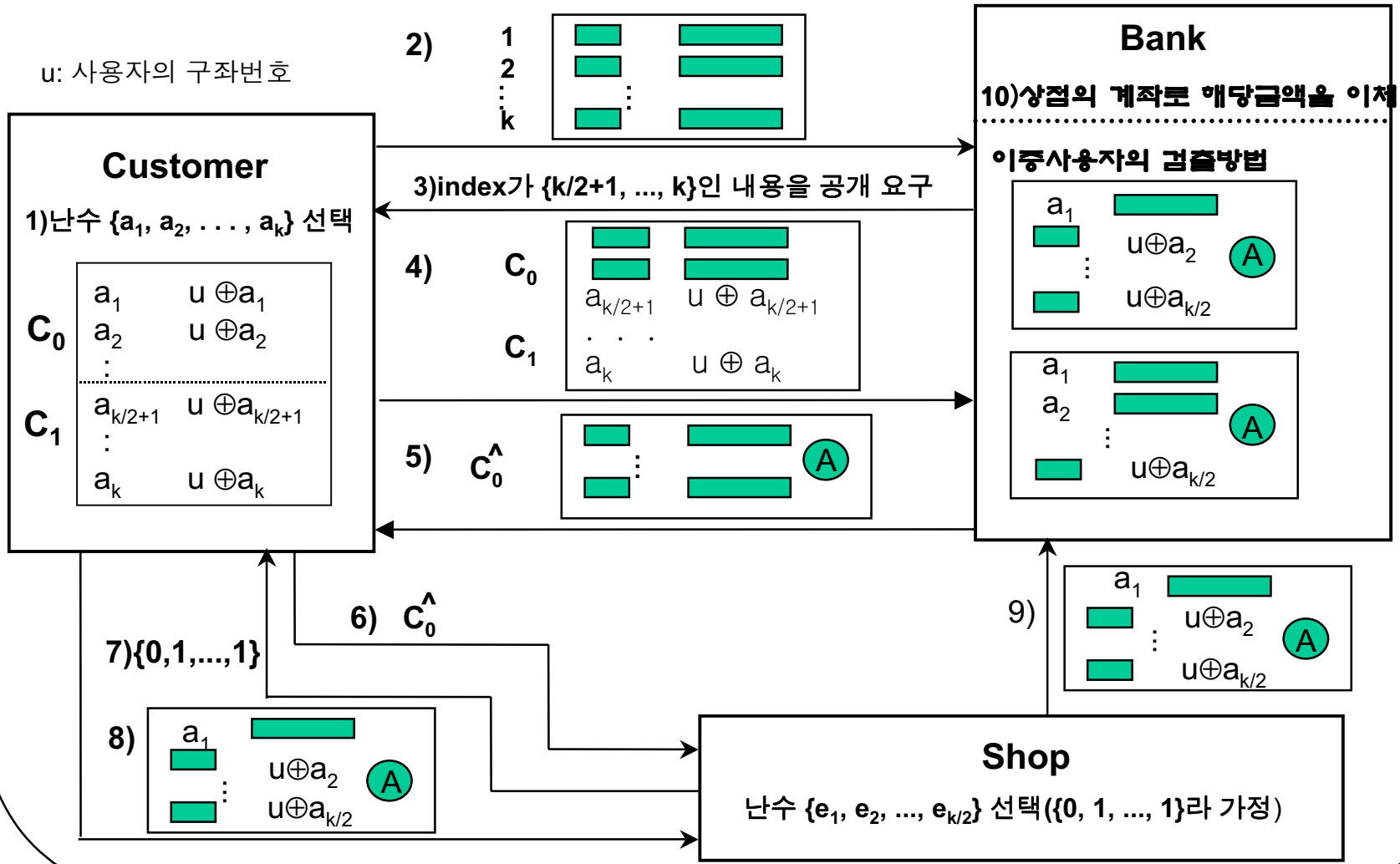


10) C의 재사용 여부를 물어봄

11) C가 재사용되지 않았으면 상점의 계좌로 해당금액을 이체

© 한국정보통신대학원 김 광조

CFN88의 오프라인 전자화폐



© 한국정보통신대학원 김 광조

CFN88의 오프라인 전자화폐(계속)

(1) 2중 사용의 검출 원리

- if e_i=1 a_i, if e_i=0 $u \oplus a_i$ 을 기억하였다가 이중 사용이 되면 $a_i \oplus u \oplus a_i = u$로 계좌 번호 찾아냄
- 은행의 질의가 2/k bit이므로 C의 이중 사용 검출 확율은 $2^{-k/2}$임

(2) 안전성

- f,g가 1-way 함수
- f(x,y) = f(x',y')이 되는 {x,y}, {x',y'}쌍을 계산 곤란

(3) 문제점

- cut and choose 방식이므로 통신량이 많다
- 타인에게 양도 불가

ZKIP(영지식 상호증명)

- GMR(Goldwasser, Micali, Rackoff) '85년도에 최초 제안
- ZKIP (Zero Knowledge Interactive Proof) : P와 V 간에
  - 완전성 (Completeness) : Only true P can prove V.
  - 건전성(Soundness) : False P' can't prove V.
  - 영 지식(0-Knowledge) : No knowledge transfer to V

© 한국정보통신대학원 김 광조

ZKIP의 개념

By Quisquater and Guillou

P knows the secret, but he doesn't want to reveal his secret.

1. V stands at point A.

2. P walks all the way into the cave, either C or D.

3. After P disappeared into the cave, V walks to point B.

4. V shouts to P asking him either to:

(a) come out of the left passage or (b) come out of the right passage

5. P complies, using the magic words to open secret door if he has to.

6. P and V repeat step (1) -(5) t times

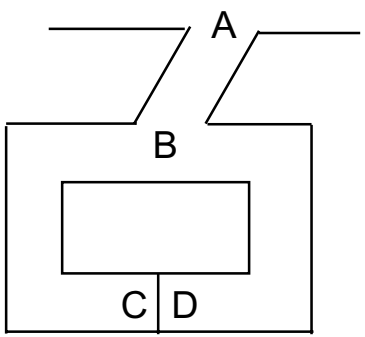


Fig.
0-knowledge cave

P knows the magic words
to open the secret door between
C and D.

© 한국정보통신대학원 김 광조

ZKIP의 방법

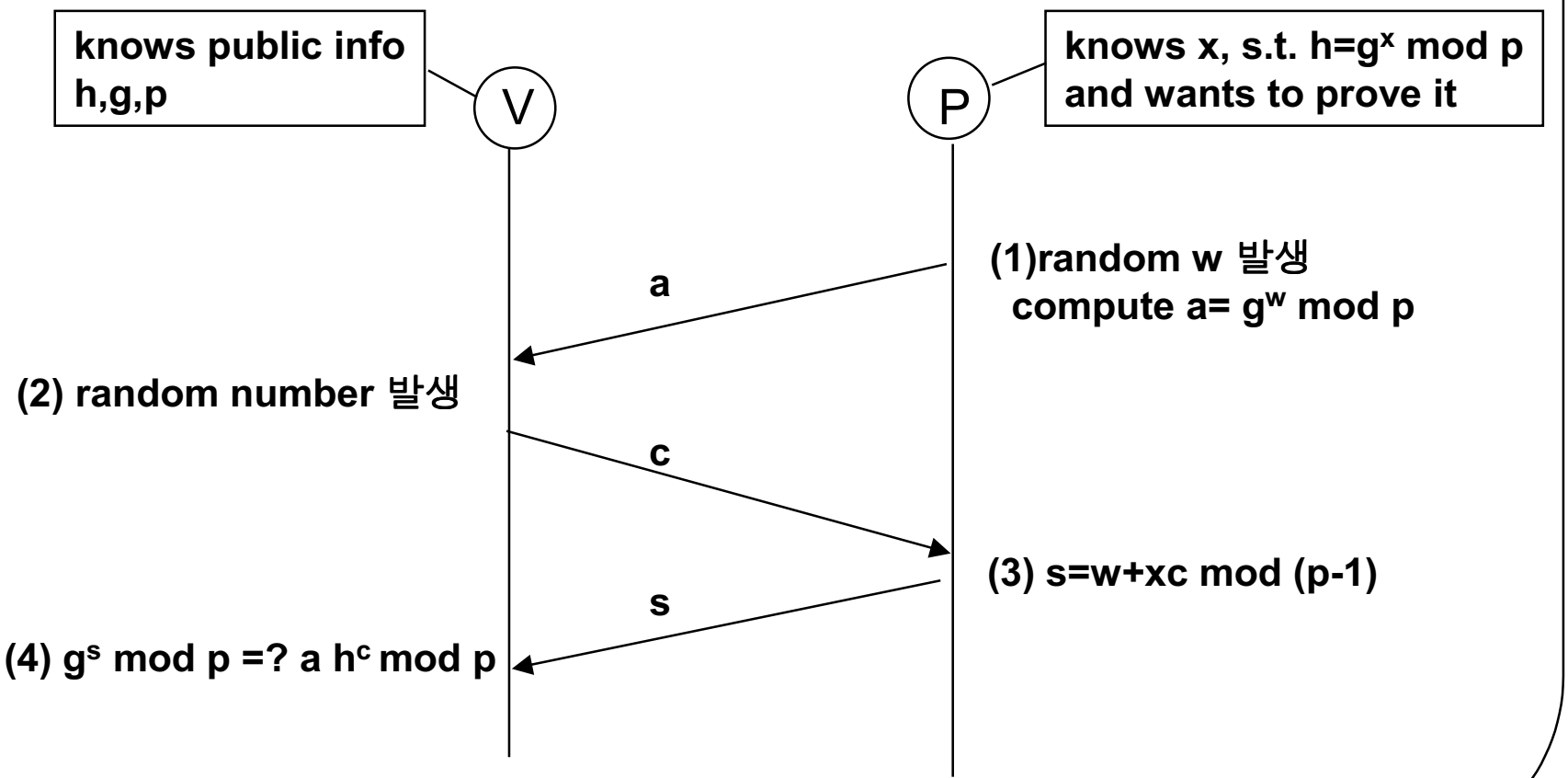
There are many ways to prove the truth of a proposition like “I know the modular square root of V” (or any other PSPACE problem):

1. To give the proof (i.e., to tell the square root to the verifier)
2. Zero-knowledge proof : to convince the verifier that the claim holds without giving him any information on the proof (and thus he cannot compute the square root).

ZKIPs are used in identification scheme, in which a user (called the prover) proves to the verifier that he knows a certain secret, without revealing the secret, or any information on the secret.

© 한국정보통신대학원 김 광조

DL-based ZKIP



© 한국정보통신대학원 김 광조

Schnorr의 본인 확인 방식

- 고객의 사전준비
  - (1) 2개의 소수 p,q, (q ¦ p-1), p=768 bits, q=140 bits
  - (2) g을 g^q=1 mod p 이 되도록 선택
  - (3) 비밀키 x < q를 선택
  - (4) 공개키 계산 $h=g^x \bmod p$
  - (5) 공개키 ={p,q,g,h}, 비밀키={x}
- 인증과정
  - (1) 고객은 난수w(<q)를 발생, $a=g^w \bmod p$를 상점에 발송
  - (2) 상점은 난수 c (0 <c < 2^t -1),t=72을 고객에 도전
  - (3) 고객은 $y=w + xc \bmod q$를 계산하여 상점으로 응답
  - (4) 상점은 g^y ?= a h^c mod p인지를 확인
- 동작이유

  x를 모르고 y를 계산하려면 $y = \log_g(g^w g^{x\,c}) \bmod p = w+xc \bmod q$ 계산은 이산 대수 문제로 귀착

© 한국정보통신대학원 김 광조

Schnorr의 본인확인 방식(예)

- 고객의 사전준비
  - (1) 2개의 소수 p=23,q=11
  - (2) $g^{11}=1 \bmod 23$ 이 되도록 g=2 선택
  - (3) 비밀키 x=9 < 11를 선택
  - (4) 공개키 계산 $h=g^x \bmod p=2^9 \bmod 23 = 6 \bmod 23$
  - (5) 공개키 ={p,q,g,h}={23,11,2,6}, 비밀키={x}={9}
- 인증과정
  - (1) 고객은 난수w=3(<q)를 발생, $a=g^w \bmod p=2^3 \bmod 23=8$를 상점에 발송
  - (2) 상점은 난수 c=3 (0 <c < 2^t -1)을 고객에 도전
  - (3) 고객은 y=w + xc mod q =3 + 9 * 5 mod q=48 mod 23=4mod23 를 계산하여 상점으로 응답
  - (4) 상점은 g^y =2^4 mod 23 =16 mod 23, a h^c mod p=8 * 6^5 mod 23=62208 mod 23=16 가 성립하여 x를 고객이 알고 있다고 판단.

Schnorr의 서명 방식

- 상점이 c를 보내는 대신에 고객이 해쉬함수 h()를 이용
- 고객의 사전 준비
  - (1) 2개의 소수 p,q, (q ¦ p-1), p=768 bits, q=140 bits
  - (2) g을 g^q=1 mod p 이 되도록 선택
  - (3) 비밀키 x < q를 선택
  - (4) 공개키 계산 $h=g^x$ mod p
  - (5) 공개키 ={p,q,g,h}, 비밀키={x}
- 디지털 서명 과정 (문서 M의 서명을 시행)
  - (1) 고객은 난수w(<q)를 발생, $a=g^w$ mod p를 계산
  - (2) 해쉬함수 h()를 이용 c=h(M¦¦a)를 계산
  - (3) 고객은 y=w + xc mod q를 계산하여 상점으로 (c,y) 및 a, M을 상점에 발송
  - (4) 상점은 g^y ?= a h^c mod p인지를 확인하고 h(M¦¦a)를 계산
  - (5) c = h(M¦¦a) 이면 서명을 승인

© 한국정보통신대학원 김 광조

Schnorr의 서명 방식(예)

- 고객의 사전준비
  - (1) 2개의 소수 p=23,q=11
  - (2) $g^{11}=1 \bmod 23$ 이 되도록 g=2 선택
  - (3) 비밀키 x=9 < 11를 선택
  - (4) 공개키 계산 $h=g^x \bmod p=2^9 \bmod 23 = 6 \bmod 23$
  - (5) 공개키 ={p,q,g,h}={23,11,2,6}, 비밀키={x}={9}
- 디지털 서명 과정 (문서 M=5의 서명을 시행)
  - (1) 고객은 난수w=3(<11)를 발생, $a=g^w \bmod p=2^3 \bmod 23=8$를 계산
  - (2) $h(k||j)=(kj)^7 \bmod 17$(좋은 해쉬함수는 아님)를 이용 $c=h(M||a)=(5*8)^7 \bmod 17=14$를 계산
  - (3) 고객은 $y=w + xc \bmod q=3+9*14 \bmod 11=8$ 를 계산하여 상점으로 (c,y)=(14,8) 및 a=8, M=5을 상점에 발송
  - (4) 상점은 $g^y \bmod p=2^8 \bmod 23=3$, $a\ h^c \bmod p=8 * 6^{14} \bmod 23=3$을 확인하고 $h(M||a)=h(5||8)=(5*8)^7 \bmod 17=14$를 계산
  - (5) c = 14, ?= h(M,a)=14 이면 서명을 승인

수학적 배경

- Z_p^*={1,2,...,p-1}상의 연산 (p:소수)
  - 곱셈에 대하여 닫혀 있음
  - 곱셈의 역원이 존재 -> 곱셈군
  - (예) Z_{11}^*={1,2,...,10}, 5*8=40=7mod11, 5*9=45=1 mod11, k
- G_q={0,1,...,q-1}상의 연산, q|p-1
- 부분군
- Fermat 정리, Lagrange 정리 등

© 한국정보통신대학원 김 광조

Representation problem

- (정의) k개의 generator $\{g_1, g_2,\ldots,g_k\}$에 대하여 ($k\geq 2$, $1 \leq a_i \leq q$, i=1 to k) 다음 식을 만족하는 h ($\in Z_q$)에 대하여 index-tuple $\{a_1,\ldots,a_k\}$를 구하는 문제

$$g_1^{a_1} g_2^{a_2} \ldots g_k^{a_k} = h \bmod p$$

- g가 Z_p^*의 부분 군 G_q의 생성원이면 DL 문제는 G_q 상에의 h에 대하여 $g^a = h \bmod p$를 만족하는 a를 구하는 것을 k개로 확장

© 한국정보통신대학원 김 광조

Representation problem(계속)

- K 개의 요소가 있으면 h를 표현하는 방법은 q^{k-1} 가지가 있다.
- (예) {2,3}이 Z_{23}^*상의 부분군 G_{11}의 생성원이면 $2^{a_1}\ 3^{a_2}=13$을 만족하는 a_1,a_2의 표현 방법은 $11^{\{2-1\}}=11$가지가 있음. $2^2*3^2=4*9=36=13 \bmod 23$, $2^7 * 3^{11}=128*1=13 \bmod 23$ 등

RP를 이용한 ZKIP

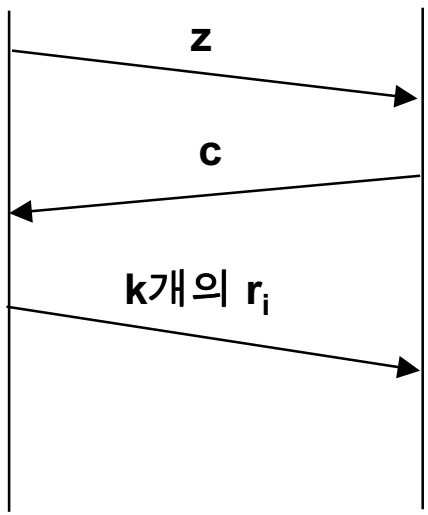
$g_1^{a1}g_2^{a2}\ldots g_k^{ak} = h \bmod p$ (RP)가 되는 $\{a_1,a_2,\ldots,a_k\}$를 알고있음.

RP가 되는 h와 $\{g_1,g_2,\ldots,g_k\}$를 알고있으나 P가 $\{a_1,\ldots,a_k\}$를 알고있는 지 확인하고 싶음

P

V

(1) G_q에 있는 k개의난수 $\{w_1,..,w_k\}$를 생성, $z=g_1^{w1}\ldots g_k^{wk} \bmod p$를 계산하여 V에게 송신



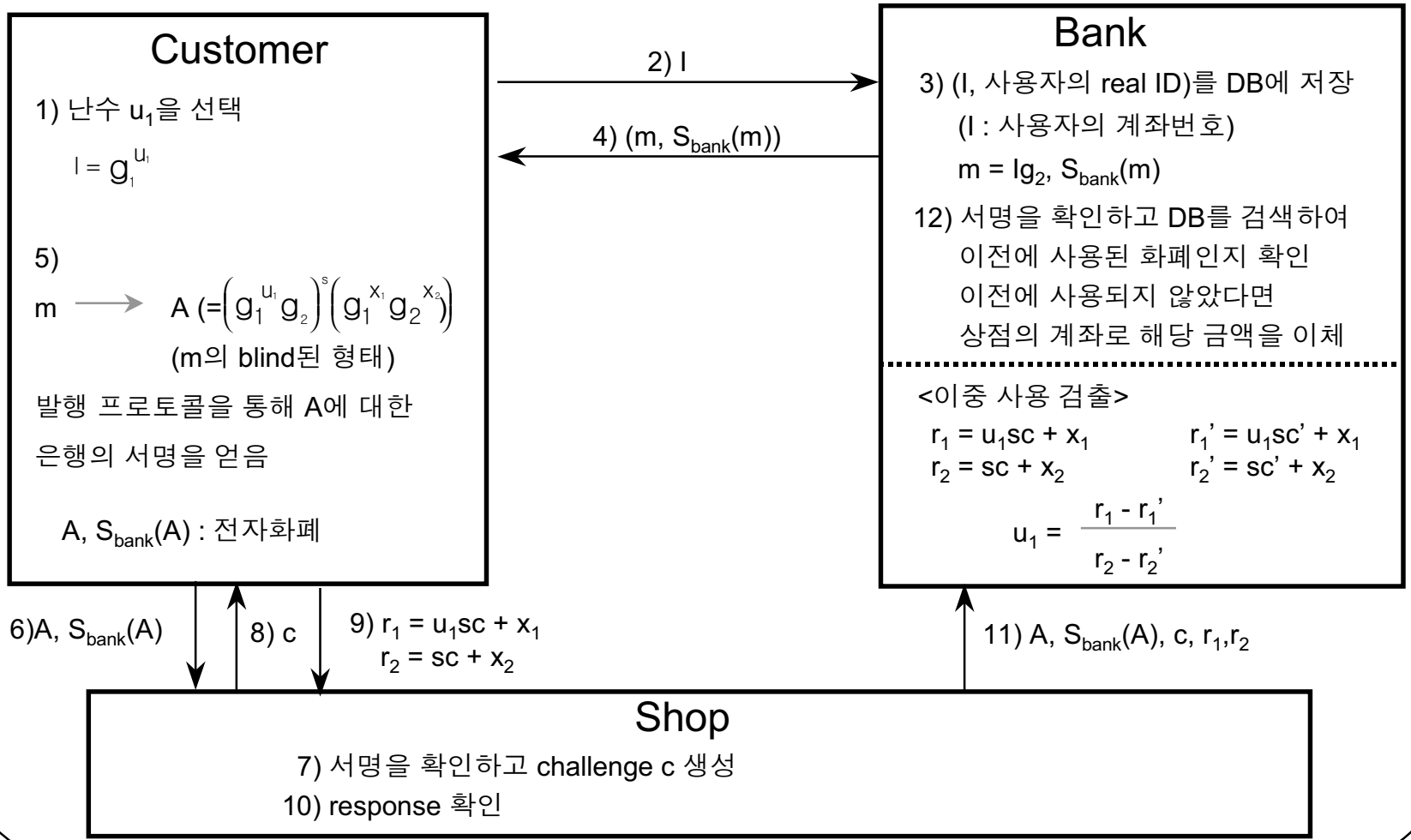
(2) 난수 c를 생성 P에게

(3) i=1에서 k까지 $r_i=a_i+c\ w_i \bmod q$를 계산 V에게 보냄

(4) $z\ h^c$를 계산하고 $g_1^{r1}\ldots g_k^{rk} \bmod p$와 같은 지 비교, 같으면 P가 $\{a_1\ldots a_k\}$를 알고 있다고 판단.

© 한국정보통신대학원 김 광조

Brands93의 전자화폐시스템



© 한국정보통신대학원 김 광조

전자 화폐의 종합

방식	기존서비스		Internet 서비스		스마트 카드 지불	
요구조건	현금	신용카드	Cyber-Cash	e-Cash	Mondex	이론형
안전성	X	X	O	O	O	{다음표
이중 사용 금지	X	X	X	O	X	참조}
프라이버시	O	X	X	O	O	
Off-line 성	O	O	O	X	O	
양도가능성	O	-	-	O	O	
분할성	X	-	-	X	O	

© 한국정보통신대학원 김 광조

전자화폐의 종합(계속)

방식 요구조건	CFN 88 전자화폐	OO91 전자화폐	Brands93 전자화폐
안전성	O	O	O
이중 사용 금지	O	O	O
프라이버시	O	O	O
Off-line 성	O	O	O
양도가능성	X	O	X
분할성	X	O	X
기본 기술	Cut&Choose	Cut&Choose/ZKIP	Challenge Response 형

© 한국정보통신대학원 김 광조

전자화폐시스템의 문제점

- ✓ 완전 범죄의 용이성(추적불가능성)
- ✓ 돈세탁이나 탈세 악용
- ✓ 양도에 따는 정보량 증가
- ✓ 통화통제의 곤란
- ✓ 블랙리스트 작성에 따른 개인의 프라이버시 침해

© 한국정보통신대학원 김 광조