BULLETPROOFS

FROM ZERO (KNOWLEDGE)
TO BULLETPROOFS

REFERENCES

- Adam Gibson, “From Zero (Knowledge) to Bulletproofs”

REFERENCES

- Groth, Jens. "Linear algebra with sub-linear zero-knowledge arguments." Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 2009.
- Bootle, Jonathan, et al. "Efficient zero-knowledge arguments for arithmetic circuits in the discrete log setting." Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2016.
- Bünz, Benedikt, et al. "Bulletproofs: Short proofs for confidential transactions and more." 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018.

BEFORE READ THE PAPER

- 표기법
  - 정수(스칼라)는 평문 소문자: x
  - 타원 곡선 상의 점은 대문자: X
  - 스칼라배(scalar multiplication)는 기호 생략: xY
  - 벡터는 굵은 글씨: $\mathbf{x}, \mathbf{X}$
  - 행렬은 mathbb: $\mathbb{X}$
  - 식 $a_1G_1 + a_2G_2 + \ldots + a_nG_n$은 두 벡터의 내적 $\mathbf{aG}$으로 표기

INTRODUCTION

INTRODUCTION

- 목표
  - “벡터를 공개하지 않고서, 연루된 커밋(commits)으로부터 알고 있음을 증명”
  - “원본을 숨기며, 커밋된 두 벡터의 내적이 0임을 증명”

INTRODUCTION

- 왜 “벡터들을 공개하지 않고서, 그 벡터들을 알고 있음을 증명”하는 것이 유용한가?
- 왜 하필이면 벡터와 내적인가?
  - 벡터의 집합을 행렬로 인코딩할 수 있음
  - 내적만이 아니라 행렬곱, 역행렬, 아다마르 곱(Hadamard product)으로 확장 가능
  - 삼각행렬(triangular matrix)인 경우에는 각종 기이(!)하고 유용한 연산 가능

COMMITMENT SCHEMES

COMMITMENT SCHEMES

- 암호학적(Cryptographic) 커미트먼트는 강력한 기술
  - 나중에 참이었음을 밝히기 전에,
  - 무엇인가를 지금은 숨긴 상태에서 참인 것으로 확약하고 싶을 때 사용

COMMITMENT SCHEMES

- 커미트먼트를 구현하는 방법 1
- 단방향 함수(one-way function)을 사용
  - 암호학적 해시 함수
  - 값 2를 커밋하고 싶으면, 2에 대한 해시를 전송:
  - “53c234e5e8472b6ac51c1ae1cab3fe06fad053beb8ebfd8977b010655bfdd3c3”

COMMITMENT SCHEMES

- 문제
  - 고작 2에 대해 “53…c3”을 전송해야 함
  - 의미상(semantic) 보안의 결핍
    - 누군가가 2와 “53…c3”의 연관성을 알아낸다면
    - 더 이상 은닉성을 제공하지 못함

COMMITMENT SCHEMES

- 커미트먼트를 구현하는 방법 2
- 무작위 값을 섞어서 커밋
    - (2 + 무작위 값) 조합을 커밋
    - $SHA256(secret\_number || random\_characters)$

COMMITMENT SCHEMES

- 커미트먼트를 구현하는 방법 2
- 무작위 값을 섞어서 커밋
  - 나중 단계에서 “값”과 "무작위 값”의 공개를 요청
  - 방법 1과 동일한 수준의 보안 속성 제공

COMMITMENT SCHEMES

- 방법 2는 커미트먼트 스킴이 가지는 주요한 두 속성을 모두 충족
  - 은닉(Hiding): 커미트먼트 C는 커밋한 값을 드러내지 않음
  - 구속(Binding): 커미트먼트 $C(m)$을 m으로부터 만든 이상,
    다른 메시지 m'으로부터 만들었다고 주장할 수 없음

COMMITMENT SCHEMES

- 문제
  - 해시 함수는 동형(homomorphic)의 특징을 갖지 않음
  - $SHA256(a) + SHA256(b) = SHA256(a + b)$가 성립하지 않음
  - 활용하기 좋은 수단이 아님
- 동형 커미트먼트 스킴은 어떻게 만들 수 있을까?

EC PEDERSEN COMMITMENT

- 타원 곡선 형태의 페더슨 커미트먼트
  - 해시 함수를 사용하는 것 대신에, 타원 곡선을 활용
- 타원 곡선계에서의 단방향 함수
  - 곡선 상의 점에 대한 스칼라배

EC PEDERSEN COMMITMENT

- 타원 곡선 상의 점에 대한 스칼라배
- $C = rH + aG$
  - C : 커미트먼트로 사용할 곡선 상의 점
  - a : 커밋할 값(숫자), r : 은닉을 제공하기 위한 무작위 값
  - G : 생성자 점
  - H : 또 다른 곡선 상의 점,
    아무도 $H = qG$를 만족하는 이산 로그 q를 몰라야 함
    (Nothing Up My Sleeve, NUMS)

EC PEDERSEN COMMITMENT

- 페더슨 커미트먼트는 동형의 특징을 가짐
  - $C(r_1, a_1) + C(r_2, a_2)$
  - $= r_1 H + a_1 G + r_2 H + a_2 G$
  - $= (r_1 + r_2)H + (a_1 + a_2)G$
  - $= C(r_1 + r_2, a_1 + a_2)$
- 커미트먼트들의 합은, 각 값의 합과 무작위 값의 합을 커미트먼트한 것과 같음

VECTOR PEDERSEN COMMITMENT

- 벡터 페더슨 커미트먼트
  - $C = rH + aG$ 를 더 강력한 형태로 확장
  - $C = rH + (v_1G_1 + v_2G_2 + \ldots + v_nG_n) = rH + \mathbf{vG}$
- 간결함에서 주된 효과
  - 벡터는 임의의 큰 숫자의 원소들로 구성될 수 있으나,
  - 오직 단 하나의 점 C에 커밋됨

VECTOR PEDERSEN COMMITMENT

- 2개 또는 더 많은 벡터를 포괄하도록 확장 가능
  - 각 벡터를 위한 N개의 NUMS 기반 곡선 상의 점만 있으면 됨
  - $C = rH + \mathbf{v}\mathbf{G} + \mathbf{w}\mathbf{H}$

ZERO KNOWLEDGE ARGUMENTS

ZERO KNOWLEDGE ARGUMENTS

- 지식 논의(Knowledge arguments)
  - 증명이 오직 계산적임을 내포
  - 지식 증명(proofs)과는 구분되는 기술 용어

ZERO KNOWLEDGE ARGUMENTS

- 영지식 증명은 확률적인 건실성을 제공하지만,
- 영지식 논의는 연산적 건실성을 제공
  - 충분한 연산 능력(매우 클 것이지만)을 가진 상대는
  - 심지어 실제로는 그렇지 않은 경우에도
  - 아마도 그가 비밀 값(들)을 알고 있다고 상대를 납득시킬 수 있음

ZERO KNOWLEDGE ARGUMENTS

- 지식 논의
  - 각자 $N(\neq m)$ 차원을 가지는 m개의 벡터 $\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_m}$
  - 각자의 커미트먼트 집합을 생성하고 나서 논할 수 있음
  - $C_1 = r_1 H + \mathbf{x_1} \mathbf{G}$
    $C_2 = r_2 H + \mathbf{x_2} \mathbf{G}$
    $\cdots$
    $C_m = r_m H + \mathbf{x_m} \mathbf{G}$

ZERO KNOWLEDGE ARGUMENTS

- 커미트먼트들은 완벽한 은닉을 제공하므로
  - 이들로부터 벡터를 알아낼 수 없음
- 이 커미트먼트들을 공유
- 이제 이들 모두를 개방할 수 있다는 영지식 관련 논의를 수행할 수 있음

ZERO KNOWLEDGE ARGUMENTS

- 영지식 논의 상호 절차
  - $P \rightarrow V : C_0$ (새롭게 선택한 N차원의 무작위 벡터에 대한 새 커미트먼트)
  - $V \rightarrow P : e$ (무작위 스칼라)
  - $P \rightarrow V : (\mathbf{z}, s)$ (N차원의 벡터와 스칼라)
- 마지막 두 값은:
  - $\mathbf{z} = \Sigma_{i=0}^{m} e^i \mathbf{x}_i$ 와 $s = \Sigma_{i=0}^{m} e^i r_i$ 로 계산
  - 덧셈(Sigma)이 0부터 시작함에 유의

ZERO KNOWLEDGE ARGUMENTS

- 어떻게 벡터 $\mathbf{x}$를 은닉시키는가?
  - $\mathbf{z}$의 한 요소 $\mathbf{z_2} = x_{02} + ex_{12} + \ldots + e^m x_{m2}$ 는
  - 벡터의 값을 덧셈으로 은닉

ZERO KNOWLEDGE ARGUMENTS

- $(\mathbf{z}, s)$를 받으면, 검증자는 이 증명이 유효한지를 다음과 같이 검증
  - 기호 =? 는 등호의 좌변과 우변이 같은지를 확인한다는 의미
  - 만일 같다면 증명은 참
  - 그렇지 않으면 증명은 거짓
- $$\sum_{i=0}^{m} e^i C_i =? \, sH + \mathbf{zG}$$

ZERO KNOWLEDGE ARGUMENTS

- 완결성(Completeness)
  - 유효성 검사의 우변을 확장:

$$
\begin{aligned}
& sH + \mathbf{z}\mathbf{G} \\
& = \sum_{i=0}^{m} e^i (r_i H) + \sum_{i=0}^{m} e^i \mathbf{x}_i \mathbf{G} \\
& = \sum_{i=0}^{m} e^i (r_i H + \mathbf{x}_i \mathbf{G}) \\
& = \sum_{i=0}^{m} e^i C_i
\end{aligned}
$$

  - 정직한 증명자는 검증자를 납득시킬 수 있음

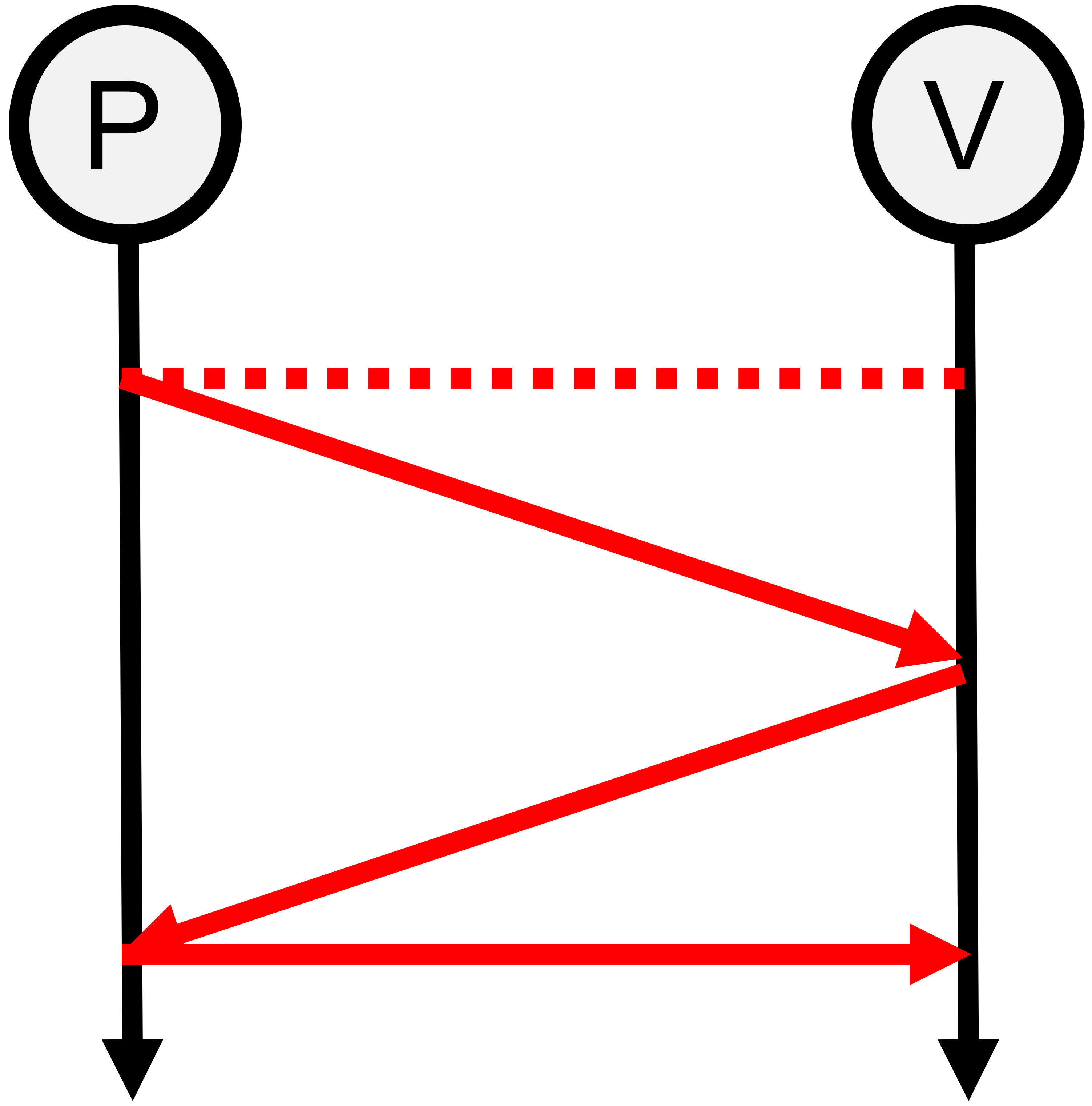
ZERO KNOWLEDGE ARGUMENTS

- 건실성(Soundness)과 영지식성(zero knowledge)
  - 생략

SIGMA PROTOCOL

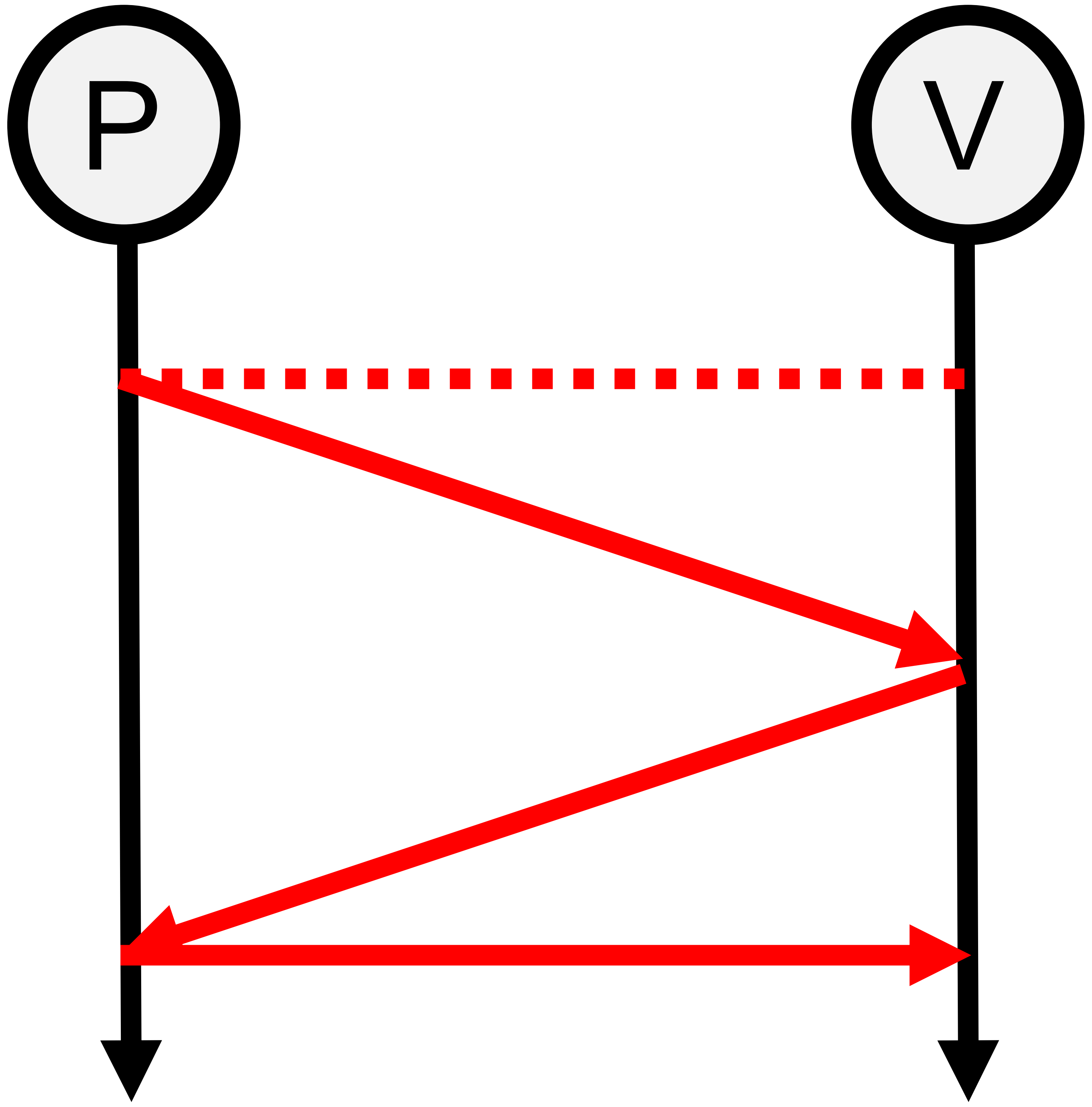
SIGMA PROTOCOL

- 상호 절차가 시그마(Σ)와 유사해 붙여진 이름
  - 증명자 —> 검증자
  - 검증자 —> 증명자
  - 증명자 —> 검증자



SIGMA PROTOCOL

- 시그마 프로토콜의 일반화
  - $P \rightarrow V$: 커미트먼트(Commitment)
  - $V \rightarrow P$: 챌린지(Challenge)
  - $P \rightarrow V$: 응답(Response) 혹은 증명(Proof)



SIGMA PROTOCOL

- 앞서 살펴본 벡터 집합의 지식 증명은
  - 시그마 프로토콜의 한 예
  - $P \rightarrow V : C_0$ (새롭게 선택한 N차원의 무작위 벡터에 대한 새 커미트먼트)
  - $V \rightarrow P : e$ (무작위 스칼라)
  - $P \rightarrow V : (\mathbf{z}, s)$ (N차원의 벡터와 스칼라)

SIGMA PROTOCOL

- 보다 간단한 예시:
- 슈노르 아이덴디티 프로토콜(Schnorr's identity protocol)
  - $P \rightarrow V : R$ (P만이 $R = kG$인 k를 알고 있는 무작위 곡선 상의 점)
  - $V \rightarrow P : e$ (무작위 스칼라)
  - $P \rightarrow V : s$ (P가 $s = ex + k$로 계산한 값)

BULLETPROOFS

FROM ZERO (KNOWLEDGE)
TO BULLETPROOFS