BULLETPROOFS

FROM ZERO (KNOWLEDGE)
TO BULLETPROOFS

INNER PROOF

INNER PROOF

- 내적 증명
    - Groth가 제시한 알고리즘
    - BulletProof의 핵심

INNER PROOF

- 내적 증명
  - 증명자가 두 벡터 $\mathbf{x}$와 $\mathbf{y}$를 가지고
  - 두 벡터의 내적 z을 명백히 알고 있는 상황

INNER PROOF

- 세 커미트먼트
  - $C_z = tH + zG$
  - $C_x = rH + \mathbf{x}\mathbf{G}$
  - $C_y = sH + \mathbf{y}\mathbf{G}$
- 증명자가 할 일은 검증자에게 다음을 납득시키는 것:
  - 세 페더슨 커미트먼트들에 대해 $z = \mathbf{x} \cdot \mathbf{y}$를 만족함

INNER PROOF

- 1. 커미트먼트 단계
- 증명자 P는 각각 $\mathbf{x}$와 $\mathbf{y}$에 상응하는
두 논스(nonce) 벡터 $\mathbf{d}_{\mathbf{x}}$, $\mathbf{d}_{\mathbf{y}}$의 커미트먼트를 전송해야 함
- 다음 페더슨 커미트먼트를 전송:

$$A_d = r_d H + \mathbf{d}_x \mathbf{G}$$
$$B_d = s_d H + \mathbf{d}_y \mathbf{G}$$

- r_d와 s_d는 무작위 값

INNER PROOF

- 1. 커미트먼트 단계
- 내적을 증명해야 하므로,
  두 숨겨진 벡터들의 내적의 커미트먼트를 전송해야 함
- 어떤 정보가 필요한가?
  - 내적의 형태가 어떻게 되는가?

INNER PROOF

- 1. 커미트먼트 단계
- 슈노르 아이덴디티 프로토콜을 상기하면:
- 임의의 챌린지 e에 대한 응답이 $e\mathbf{x} + \mathbf{d}_{\mathbf{x}}$, $e\mathbf{y} + \mathbf{d}_{\mathbf{y}}$ 형태일 것임을 직관적으로 예상할 수 있음
  - 슈노르 아이덴디티 프로토콜에서 $ex + k$에 해당

INNER PROOF

- 1. 커미트먼트 단계
- 숨겨진 형태 $e\mathbf{x} + \mathbf{d}_\mathbf{x}$, $e\mathbf{y} + \mathbf{d}_\mathbf{y}$의 내적 $((e\mathbf{x} + \mathbf{d}_\mathbf{x})\cdot(e\mathbf{y} + \mathbf{d}_\mathbf{y}))$은 e에 대한 이차식의 형태
    - 3개의 계수(coefficients)를 가짐
    - 계수에 대한 커미트먼트를 제공해야 함

INNER PROOF

- 1. 커미트먼트 단계
- e^2에 대한 계수는 이미 $C_z = tH + zG$, $z = \mathbf{x} \cdot \mathbf{y}$로 주어져 있음
- 따라서 2개만 더 추가로 제공하면 됨
  - $C_1 = t_1 H + (\mathbf{x} \cdot \mathbf{d_y} + \mathbf{y} \cdot \mathbf{d_x})G$
  - $C_0 = t_0 H + (\mathbf{d_x} \cdot \mathbf{d_y})G$

INNER PROOF

- 1. 커미트먼트 단계
- 결론적으로 본 커미트먼트 단계에서 증명자는
  - 4개의 무작위 스칼라 r_d, s_d, t_1, t_0 와
  - 2개의 무작위 벡터 $\mathbf{d_x}, \mathbf{d_y}$ 를 생성
- 이들로부터 생성한 4개의 페더슨 커미트먼트
  - A_d, B_d, C_1, C_0 를 전송

INNER PROOF

- 2. 챌린지 단계
- 검증자가 하나의 스칼라 e를 전송

INNER PROOF

- 3. 응답 단계
- 응답 단계에서 증명자는 다음과 같은 값들을 전송
- $$\mathbf{f}_x = e\mathbf{x} + \mathbf{d}_x$$
  $$\mathbf{f}_y = e\mathbf{y} + \mathbf{d}_y$$
  $$r_x = er + r_d$$
  $$s_y = es + s_d$$
  $$t_z = e^2 t + e t_1 + t_0$$

INNER PROOF

- 3. 응답 단계
- 두 벡터의 숨겨진 형태 $\mathbf{f}_x, \mathbf{f}_y$ 에 대해
  검증자는 커미트먼트를 복구하고 C_x, C_y와 일치하는지 검증
- $eC_x + A_d =?\, r_x H + \mathbf{f}_x \mathbf{G}$
  $eC_y + B_d =?\, s_y H + \mathbf{f}_y \mathbf{G}$

INNER PROOF

- 3. 응답 단계
- r_x, s_y는 상응하는 페더슨 커미트먼트에 대해
- 무작위 값을 만들기 위해 사용됨

INNER PROOF

- 3. 응답 단계
- 마지막으로, t_z에 대한 검증이 필요
    - 이 검증으로부터 내적이 올바르다는 것을 확인
    - 페더슨 커미트먼트 식의 무작위 값이 올바르다는 것을 확인

INNER PROOF

- 3. 응답 단계
- $\mathbf{f_x} \cdot \mathbf{f_y}$
  $= (e\mathbf{x} + \mathbf{d_x}) \cdot (e\mathbf{y} + \mathbf{d_y})$
  $= e^2 z + e(\mathbf{x} \cdot \mathbf{d_y} + \mathbf{y} \cdot \mathbf{d_x}) + \mathbf{d_x} \cdot \mathbf{d_y}$
  - ($z = \mathbf{x} \cdot \mathbf{y}$ 이므로)

INNER PROOF

- 3. 응답 단계
- 페더슨 커미트먼트 $Comm$에 대해 위 식은
- $Comm(\mathbf{f_x} \cdot \mathbf{f_y})$
  $= e^2 C_z + e(Comm((\mathbf{x} \cdot \mathbf{d_y} + \mathbf{y} \cdot \mathbf{d_x})) + Comm(\mathbf{d_x} \cdot \mathbf{d_y})$
- 준비해둔 C_1, C_0, t_z 에 따라:
- $t_z H + (\mathbf{f}_x \cdot \mathbf{f}_y)G =? \, e^2 C_z + eC_1 + C_0$

INNER PROOF

- 완결성
- $eC_x + A_d =? \, r_x H + \mathbf{f}_x \mathbf{G}$ 에 대해:
  $eC_y + B_d =? \, s_y H + \mathbf{f}_y \mathbf{G}$
- $$\begin{aligned} & eC_x + A_d \\ &= e(rH + \mathbf{x}\mathbf{G}) + r_d H + \mathbf{d}_x \mathbf{G} \\ &= (er + r_d)H + (e\mathbf{x} + \mathbf{d}_x)\mathbf{G} \\ &= r_x H + \mathbf{f}_x \mathbf{G} \end{aligned}$$

$$\begin{aligned} & eC_y + B_d \\ &= e(sH + \mathbf{y}\mathbf{G}) + s_d H + \mathbf{d}_y \mathbf{G} \\ &= (es + s_d)H + (e\mathbf{y} + \mathbf{d}_y)\mathbf{G} \\ &= s_y H + \mathbf{f}_y \mathbf{G} \end{aligned}$$

INNER PROOF

- 완결성
- $t_z H + (\mathbf{f}_x \cdot \mathbf{f}_y) G =? \, e^2 C_z + e C_1 + C_0$ 에 대해:

$$
\begin{aligned}
& e^2 C_z + e C_1 + C_0 \\
& = e^2 (tH + zG) + \mathrm{e}\big(t_1 H + (\mathbf{x} \cdot \mathbf{d}_y + \mathbf{y} \cdot \mathbf{d}_x) G\big) + \big(t_0 H + (\mathbf{d}_x \cdot \mathbf{d}_y) G\big) \\
& = (e^2 t + e t_1 + t_0) H + \big(e^2 z + e(\mathbf{x} \cdot \mathbf{d}_y + \mathbf{y} \cdot \mathbf{d}_x) + \mathbf{d}_x \cdot \mathbf{d}_y\big) G \\
& = (e^2 t + e t_1 + t_0) H + (e\mathbf{x} + \mathbf{d}_x) \cdot (e\mathbf{y} + \mathbf{d}_y) G \\
& = t_z H + (\mathbf{f}_x \cdot \mathbf{f}_y) G
\end{aligned}
$$

- 따라서 정직한 증명자는 검증자를 납득시킬 수 있음

MORE COMPACT INNER PROOF

MORE COMPACT INNER PROOF

- 더 간결한 내적 증명
  - Bootle의 논문에서
- 내적 증명 문제를 해결하기 위한 더 정교하고 현명한 방법 제시
  - 재귀(recursion)의 도입
- BulletProof에서 사용되는 아이디어와 매우 유사

MORE COMPACT INNER PROOF

- 목적은 두 당사자(증명자와 검증자) 사이의
- 데이터 통신의 양을 줄이는 것
    - 피아트-샤미르 휴리스틱(Fiat-Shamir heuristic)을 사용해 비-상호작용 형태로 바꾸면 더 간결한 증명이 됨 (생략)
- 영지식에 대한 새로운 방법이 아닌
- 연산에 이점이 있는 방법을 제시

MORE COMPACT INNER PROOF

- 하나의 벡터에 대한 고려
- 어떠한 벡터의 커미트먼트를 만들고 증명을 전송하는 데 얼마나 많은 데이터가 필요한가?

MORE COMPACT INNER PROOF

- 하나의 벡터에 대한 고려
- 10차원의 벡터 $\mathbf{a} = [a_1, a_2, \ldots, a_{10}]$ 의 예시:
  - 페더슨 커미트먼트를 사용
  - 무작위 값은 없다고 가정
  - $A = a_1G_1 + a_2G_2 + \ldots + a_{10}G_{10}$

MORE COMPACT INNER PROOF

- $A = a_1G_1 + a_2G_2 + \ldots + a_{10}G_{10}$
- $[a_1, a_2, \ldots, a_{10}]$을 공개하는 것으로 지식 증명이 가능
  - 정보가 공개됨
  - 10개의 스칼라를 전송해야 함
  - 타원곡선 시나리오에서는 스칼라 각자가 32바이트에 해당함
- 압축시킬 방법은 없을까?

MORE COMPACT INNER PROOF

- $A = a_1G_1 + a_2G_2 + \ldots + a_{10}G_{10}$
- 현명한 방법은 커미트먼트 A를 다른 커미트먼트 A'으로 바꾸는 것
  - 벡터의 원소 개수를 줄임으로써 형성
  - 그럼에도 불구하고 원래의 커미트먼트를 내포해야 함

MORE COMPACT INNER PROOF

- 커미트먼트 단계
- 원본 벡터를 조각으로 나눔
  - $[a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}] = [[a_1, a_2], [a_3, a_4], [a_5, a_6], [a_7, a_8], [a_9, a_{10}]]$
- 동일한 연산을 G_i 들에 대해서도 수행

MORE COMPACT INNER PROOF

- 커미트먼트 단계
- 식의 우변을 5개의 2차원 벡터로 취급:
  - $[a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}] = [[a_1, a_2], [a_3, a_4], [a_5, a_6], [a_7, a_8], [a_9, a_{10}]]$ 에서
  - $[[a_1, a_2], [a_3, a_4], [a_5, a_6], [a_7, a_8], [a_9, a_{10}]] = [\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \mathbf{a}_4, \mathbf{a}_5]$
- G에 관한 부분 역시:
  - $[\mathbf{G}_1, \mathbf{G}_2, \mathbf{G}_3, \mathbf{G}_4, \mathbf{G}_5]$

MORE COMPACT INNER PROOF

- 커미트먼트 단계
- 본 예제에서는 10=5X2 라서 두 개씩 묶었지만
- 개수는 소인수분해에 따라 달라질 수 있음
    - 가령 21개로 시작했으면 21=7X3이니 세 개씩 묶으면 됨

MORE COMPACT INNER PROOF

- 커미트먼트 단계
- 새로운 배치를 행렬 형태로 시각화 할 수 있음
- $$\begin{pmatrix} \mathbf{a_1 G_1} & \mathbf{a_2 G_1} & \cdots & \cdots & \mathbf{a_5 G_1} \\ \mathbf{a_1 G_2} & \mathbf{a_2 G_2} & \cdots & \cdots & \cdots \\ \cdots & \cdots & \mathbf{a_3 G_3} & \cdots & \cdots \\ \cdots & \cdots & \cdots & \mathbf{a_4 G_4} & \cdots \\ \mathbf{a_1 G_5} & \cdots & \cdots & \cdots & \mathbf{a_5 G_5} \end{pmatrix}$$

MORE COMPACT INNER PROOF

- 커미트먼트 단계
- $$\begin{pmatrix} \mathbf{a}_1\mathbf{G}_1 & \mathbf{a}_2\mathbf{G}_1 & \ldots & \ldots & \mathbf{a}_5\mathbf{G}_1 \\ \mathbf{a}_1\mathbf{G}_2 & \mathbf{a}_2\mathbf{G}_2 & \ldots & \ldots & \ldots \\ \ldots & \ldots & \mathbf{a}_3\mathbf{G}_3 & \ldots & \ldots \\ \ldots & \ldots & \ldots & \mathbf{a}_4\mathbf{G}_4 & \ldots \\ \mathbf{a}_1\mathbf{G}_5 & \ldots & \ldots & \ldots & \mathbf{a}_5\mathbf{G}_5 \end{pmatrix}$$
- 행렬의 주대각성분의 합이 A임
  - $\mathbf{a}_i\mathbf{G}_i = a_{2i-1}G_{2i-1} + a_{2i}G_{2i} \;\; \forall i \in 1..5$

MORE COMPACT INNER PROOF

- 커미트먼트 단계
- 전송해야 하는 커미트먼트들의 개수는
  - 이미 알고있는 주대각성분 A를 포함해 2X5-1 = 9개
- 대각성분에 관한 수식:
  - $-4 \le k \le 4$ 인 정수 k에 대해 $A_k = \sum_{\max(1,1-k)}^{\min(5,5-k)} \mathbf{a}_{i+k}\mathbf{G}_i$
- 커미트먼트의 수를 9개로 줄임

MORE COMPACT INNER PROOF

$$
\begin{pmatrix}
\mathbf{a}_1\mathbf{G}_1 & \mathbf{a}_2\mathbf{G}_1 & \mathbf{a}_3\mathbf{G}_1 & & \mathbf{a}_5\mathbf{G}_1 \\
\mathbf{a}_1\mathbf{G}_2 & \mathbf{a}_2\mathbf{G}_2 & \mathbf{a}_3\mathbf{G}_2 & \cdots & \mathbf{a}_5\mathbf{G}_2 \\
\mathbf{a}_1\mathbf{G}_3 & \mathbf{a}_2\mathbf{G}_3 & \mathbf{a}_3\mathbf{G}_3 & & \mathbf{a}_5\mathbf{G}_3 \\
 & \vdots & & \ddots & \vdots \\
\mathbf{a}_1\mathbf{G}_5 & \mathbf{a}_2\mathbf{G}_5 & \mathbf{a}_3\mathbf{G}_5 & \cdots & \mathbf{a}_5\mathbf{G}_5
\end{pmatrix}
$$

$$
\begin{aligned}
A_{-4} &= \mathbf{a}_1\mathbf{G}_5 \\
A_{-3} &= \mathbf{a}_1\mathbf{G}_4 + \mathbf{a}_2\mathbf{G}_5 \\
A_{-2} &= \mathbf{a}_1\mathbf{G}_3 + \mathbf{a}_2\mathbf{G}_4 + \mathbf{a}_3\mathbf{G}_5 \\
A_{-1} &= \mathbf{a}_1\mathbf{G}_2 + \mathbf{a}_2\mathbf{G}_3 + \mathbf{a}_3\mathbf{G}_4 + \mathbf{a}_4\mathbf{G}_5 \\
A_0 &= \mathbf{a}_1\mathbf{G}_1 + \mathbf{a}_2\mathbf{G}_2 + \mathbf{a}_3\mathbf{G}_3 + \mathbf{a}_4\mathbf{G}_4 + \mathbf{a}_5\mathbf{G}_5 \\
A_1 &= \mathbf{a}_2\mathbf{G}_1 + \mathbf{a}_3\mathbf{G}_2 + \mathbf{a}_4\mathbf{G}_3 + \mathbf{a}_5\mathbf{G}_4 \\
A_2 &= \mathbf{a}_3\mathbf{G}_1 + \mathbf{a}_4\mathbf{G}_2 + \mathbf{a}_5\mathbf{G}_3 \\
A_3 &= \mathbf{a}_4\mathbf{G}_1 + \mathbf{a}_5\mathbf{G}_2 \\
A_4 &= \mathbf{a}_5\mathbf{G}_1
\end{aligned}
$$

MORE COMPACT INNER PROOF

- 챌린지 단계
- 검증자가 하나의 스칼라 x를 전송

MORE COMPACT INNER PROOF

- 압축 단계
- 실질적인 압축이 일어나는 지점
- 다음과 같은 새로운 2차원 벡터들을 형성:

$$\mathbf{a}' = \sum_{i=1}^{5} x^{i}\mathbf{a}_i\,, \qquad \mathbf{G}' = \sum_{i=1}^{5} x^{-i}\mathbf{G}_i$$

MORE COMPACT INNER PROOF

- 압축 단계
- $\mathbf{G}'$ 은 명시적으로 다음과 같음:

$$\begin{aligned}\mathbf{G}' &= (G'_1, G'_2)\\ &= [x^{-1}G_1, x^{-1}G_2] + [x^{-2}G_3, x^{-2}G_4] + [x^{-3}G_5, x^{-3}G_6] + [x^{-4}G_7, x^{-4}G_8] + [x^{-5}G_9, x^{-5}G_{10}]\\ &= [(x^{-1}G_1 + x^{-2}G_3 + x^{-3}G_5 + x^{-4}G_7 + x^{-5}G_9), (x^{-1}G_2 + x^{-2}G_4 + x^{-3}G_6 + x^{-4}G_8 + x^{-5}G_{10})]\end{aligned}$$

- $\mathbf{a}'$ 에 대해서 x의 지수가 양수인 점만 제외하면 유사:

$$\begin{aligned}&\mathbf{a}'\\ &= [(xa_1 + x^2a_3 + x^3a_5 + x^4a_7 + x^5a_9), (xa_2 + x^2a_4 + x^3a_6 + x^4a_8 + x^5a_{10})]\end{aligned}$$

MORE COMPACT INNER PROOF

- 압축 단계
- 커미트먼트를 이 새로운 좌표계로 치환:

$$A' = \mathbf{a}'\mathbf{G}'$$
$$= (xa_1 + x^2a_3 + x^3a_5 + x^4a_7 + x^5a_9)G_1' + (xa_2 + x^2a_4 + x^3a_6 + x^4a_8 + x^5a_{10})G_2'$$

  - G_1', G_2'는 2차원 벡터 $\mathbf{G}'$의 두 원소
- 위 식의 곱셈항을 전개해 행렬꼴로 나타낼 수 있음

MORE COMPACT INNER PROOF

- 압축 단계
- 곱셈항을 전개해 행렬꼴로 나타낼 수 있음

$$\begin{pmatrix} a_1G_1 + a_2G_2 & x(a_3G_1 + a_4G_2) & x^2(a_5G_1 + a_6G_2) & x^3(a_7G_1 + a_8G_2) & x^4(a_9G_1 + a_{10}G_2) \\ x^{-1}(a_1G_3 + a_2G_4) & a_3G_3 + a_4G_4 & x(a_5G_3 + a_6G_4) & x^2(a_7G_3 + a_8G_4) & x^4(a_9G_3 + a_{10}G_4) \\ \ldots & \ldots & a_5G_5 + a_6G_6 & \ldots & \ldots \\ \ldots & \ldots & \ldots & a_7G_7 + a_8G_8 & \ldots \\ x^{-4}(a_1G_9 + a_2G_{10}) & \ldots & \ldots & \ldots & a_9G_9 + a_{10}G_{10} \end{pmatrix}$$

  - 주대각성분의 합이 $A = a_1G_1 + a_2G_2 + \ldots + a_{10}G_{10}$ 과 같음
  - 대각성분은 같은 지수를 가진 x 항들이 모여있음

MORE COMPACT INNER PROOF

- 압축 단계
- A와 A'를 연관짓기 위해 검증자는 전체 항을 검증해야 함
- 다음을 계산:
  - $$A' = \sum_{k=-4}^{4} x^k A_k$$
  - $$A' = \sum_{k=-4}^{4} x^k A_k = \sum_{k=-4}^{4} \sum_{\max(1,1-k)}^{\min(5,5-k)} x^k \mathbf{a}_{i+k} \mathbf{G}_i$$

MORE COMPACT INNER PROOF

- 재귀 단계
- 증명자와 검증자 모두 A' 및 G'을 구성할 수 있음이 핵심
  - 예시에서 10차원의 벡터 $\mathbf{a}$로 시작했으며
  - 현재 2차원의 벡터 $\mathbf{a}'$을 다루고 있음에 주목
  - 현재 벡터 $\mathbf{a}'$ 그 자체는 증명자만이 알고 있음

MORE COMPACT INNER PROOF

- 재귀 단계
- 만일 600차원의 벡터로 시작했다면?
  - 60 X 10 으로 간주해 $\mathbf{G}'$ 은 60차원을 가짐
- 재귀적으로, 60차원의 $\mathbf{G}'$ 을
  - 6 X 10 으로 간주해 압축
  - 6차원의 벡터 10개

MORE COMPACT INNER PROOF

- 재귀 단계
- $A \leftarrow A', G \leftarrow G'$ 으로
  - 커미트먼트 단계
  - 챌린지 단계
  - 압축 단계를 반복

MORE COMPACT INNER PROOF

- 공개 단계
- 여러 재귀 단계를 거쳐 마지막 단계에 다다르면
  - 증명자는 해당 벡터를 공개
  - 예시에서는 두 개의 숫자로 구성된 벡터 $\mathbf{a}'$ 를 공개
    - $[(xa_1 + x^2a_3 + x^3a_5 + x^4a_7 + x^5a_9), (xa_2 + x^2a_4 + x^3a_6 + x^4a_8 + x^5a_{10})]$

MORE COMPACT INNER PROOF

- 요약) 공시된 커미트먼트 A에 대한 상호작용의 패턴
  - 커미트먼트 단계: P가 대각성분 커미트먼트를 전송
  - 챌린지 단계: V가 x를 전송
  - 압축 단계: 양 측이 $A', \mathbf{G}'$을 계산
  - 재귀 단계: (1) $A \leftarrow A', \mathbf{G} \leftarrow \mathbf{G}'$. (2) P가 새로운 대각성분 커미트먼트를 전송 .
    (3) V가 x'을 전송 . (4) (1)~(3)의 반복 .
  - 공개 단계: P가 벡터 $\mathbf{a}'$을 공개

MORE COMPACT INNER PROOF

- 얼마나 (압축에) 도움이 되는가?
- 10차원의 경우
  - 주대각성분의 커미트먼트 A를 제외하고
  - 추가적인 8 = 9 - 1 개의 커미트먼트를 전송해야 함
  - 마지막에 2개의 스칼라를 공개
  - 대략 10개의 스칼라 전송과 비슷한 수준

MORE COMPACT INNER PROOF

- 얼마나 (압축에) 도움이 되는가?
- 600차원의 경우
  - 60차원의 벡터 10개로 압축, 6차원의 벡터 10개로 압축
  - 마지막에는 단지 6개의 스칼라
  - 각 압축 단계에서 2 X 10 - 1 = 19 커미트먼트가 발생
  - 총 2 X 19 + 6 - 1 = 43 개만 전송하면 됨
- 600차원을 그대로 전송하려면 600개의 스칼라를 전송해야 했음

MORE COMPACT INNER PROOF

- 지금까지는 하나의 벡터 $\mathbf{a}$에 대해서만 고려함
  - 내적 증명으로 확장
  - 일반적인 지식 증명: $z = \mathbf{a} \cdot \mathbf{b}$인 $\mathbf{a}$, $\mathbf{b}$, z에 관해 적용

MORE COMPACT INNER PROOF

- 10차원 벡터의 예로, 벡터 $\mathbf{b}$를 고려
  - 위의 방법을 그대로 적용
  - 단, $\mathbf{G}$를 다른 곡선 상의 점들을 대표하는 $\mathbf{H}$로 대체
  - 챌린지 x를 역수(inverse)인 x^{-1}로 적용
- $$B' = \sum_{k=-4}^{4} x^{-k} B_k$$

MORE COMPACT INNER PROOF

- $z = \mathbf{a} \cdot \mathbf{b}$ 에서
  - 두 벡터 모두 압축된 형태
  - 즉, $\mathbf{a} = [\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \mathbf{a}_4, \mathbf{a}_5]$, $\mathbf{b} = [\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4, \mathbf{b}_5]$
  - $\mathbf{a} \cdot \mathbf{b}$를 행렬 꼴로 나타내면: $\begin{pmatrix} \mathbf{a}_1\mathbf{b}_1 & \mathbf{a}_2\mathbf{b}_1 & \ldots & \ldots & \mathbf{a}_5\mathbf{b}_1 \\ \mathbf{a}_1\mathbf{b}_2 & \mathbf{a}_2\mathbf{b}_2 & \ldots & \ldots & \ldots \\ \ldots & \ldots & \mathbf{a}_3\mathbf{b}_3 & \ldots & \ldots \\ \ldots & \ldots & \ldots & \mathbf{a}_4\mathbf{b}_4 & \ldots \\ \mathbf{a}_1\mathbf{b}_5 & \ldots & \ldots & \ldots & \mathbf{a}_5\mathbf{b}_5 \end{pmatrix}$

MORE COMPACT INNER PROOF

- $\mathbf{a}' = \Sigma_{i=1}^{5} x^i \mathbf{a_i}$ 와 마찬가지로 $\mathbf{b}'$ 은:
  - 챌린지를 x^{-1}로 적용했음에 유의
  - $$\mathbf{b}' = \sum_{i=1}^{5} x^{-i} \mathbf{b}_i$$

MORE COMPACT INNER PROOF

- z'과 z_k를 구성함:
  - $$z' = \sum_{k=-4}^{4} z_k x^k, \qquad z_k = \sum_{\max(1,1-k)}^{\min(5,5-k)} \mathbf{a}_{i+k} \cdot \mathbf{b}_i \ \ (\text{for } -4 \le k \le 4)$$

MORE COMPACT INNER PROOF

- $z' = \mathbf{a}' \cdot \mathbf{b}'$ 임을 보이기는 쉬움
  - $\mathbf{a}' = \left[(xa_1 + x^2a_3 + x^3a_5 + x^4a_7 + x^5a_9), \left((xa_2 + x^2a_4 + x^3a_6 + x^4a_8 + x^5a_{10})\right)\right]$
    $\mathbf{b}' = \left[(x^{-1}b_1 + x^{-2}b_3 + x^{-3}b_5 + x^{-4}b_7 + x^{-5}b_9), \left((x^{-1}b_2 + x^{-2}b_4 + x^{-3}b_6 + x^{-4}b_8 + x^{-5}b_{10})\right)\right]$
  - $\mathbf{a}' \cdot \mathbf{b}'$
    $= (xa_1 + x^2a_3 + x^3a_5 + x^4a_7 + x^5a_9)(x^{-1}b_1 + x^{-2}b_3 + x^{-3}b_5 + x^{-4}b_7 + x^{-5}b_9) +$
    $(xa_2 + x^2a_4 + x^3a_6 + x^4a_8 + x^5a_{10})(x^{-1}b_2 + x^{-2}b_4 + x^{-3}b_6 + x^{-4}b_8 + x^{-5}b_{10})$
    $= a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4 + a_5b_5 + x^{-4}(\dots) + \cdots + x^4(\dots)$
    $= z'$

MORE COMPACT INNER PROOF

- 요약) 벡터 각각은 물론이고 내적에 대해서도 간결한 증명 작업을 수행할 수 있음
  - 벡터 $\mathbf{G}, \mathbf{H}$는 이미 설정되었다고 가정
  - 증명자가 초기에 (A, B, z)를 공시
  - A와 B는 커미트먼트이며, $z = \mathbf{a} \cdot \mathbf{b}$를 만족
  - 벡터는 임의의 차원 $n = m_1 \times m_2 \times \ldots$

MORE COMPACT INNER PROOF

- 커미트먼트 단계: P가 인수 m_2에 대해 대각성분 커미트먼트 $(A_k, B_k, z_k \forall k \in (1-m)..(m-1))$을 전송
- 챌린지 단계: V가 x를 전송
- 압축 단계: 양 측이 $A', B', z', \mathbf{G}', \mathbf{H}'$ 을 계산
- 재귀 단계: (1) $A \leftarrow A', B \leftarrow B', z \leftarrow z', \mathbf{G} \leftarrow \mathbf{G}', \mathbf{H} \leftarrow \mathbf{H}'$
  (2) P가 다른 인수 m_3에 대해 새로운 대각성분 커미트먼트를 전송
  (3) V가 x'을 전송 . 반복 .
- 공개 단계: P가 벡터 $\mathbf{a}'$ 과 $\mathbf{b}'$ 을 공개함. 이 둘의 내적은 z' 임

BULLETPROOFS

FROM ZERO (KNOWLEDGE)
TO BULLETPROOFS