Position Based Cryptography

Nishanth Chandran Vipul Goyal Ryan Moriarty Rafail Ostrovsky

UCLA

What constitutes an identity?

- Your public key

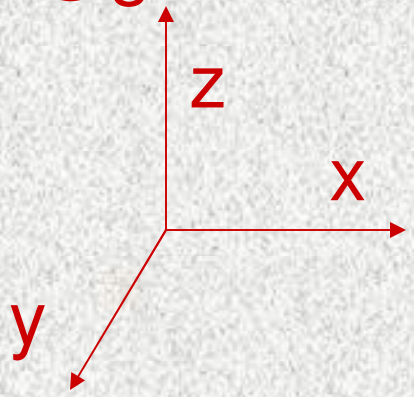
PK

- Your biometric

- Email ID

abc@gmail.com

- How about where you are?



Geographical Position as an Identity

sk **sk**

$Enc_{sk}(m)$

US Military Base in USA → **US Military Base in Iraq**

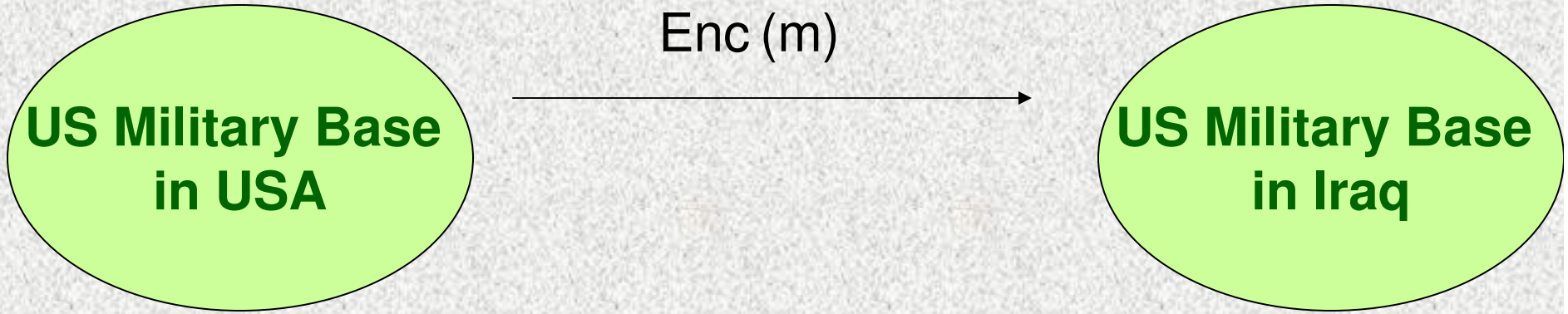
Geographical Position as an Identity

US Military Base in USA

US Military Base in Iraq

- **We trust physical security**
- **Guarantee that those inside a particular geographical region are good**

Geographical Position as an Identity



Only someone at a particular geographical position can decrypt

Other Applications

- *Position-based Authentication*: guarantee that a message came from a person at a particular geographical position
- *Position-based access control*: allow access to resource only if user is at particular geographical position

Many more….

Problem (informally)

- A set of verifiers present at various geographical positions in space
- A prover present at some geographical position P

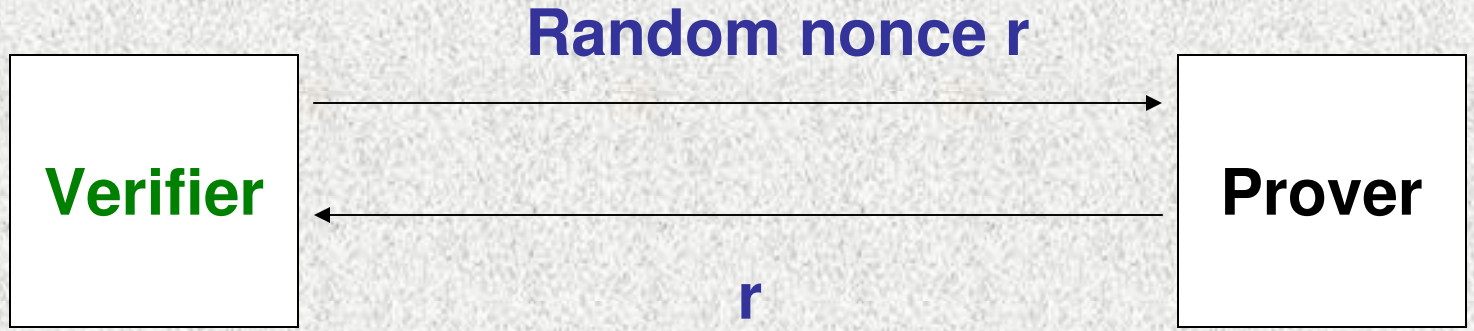
GOAL: Exchange a key with the prover if and only if prover is in fact at position P

Secure Positioning

- Set of verifiers wish to verify the position claim of a prover at position P
- Run an interactive protocol with the prover at P to verify this
- Studied in wireless security
  [SSW03, B04, SP05, CH05, CCS06]

Previous Techniques for Secure Positioning

All messages travel at speed of light
Radio waves, GPS….

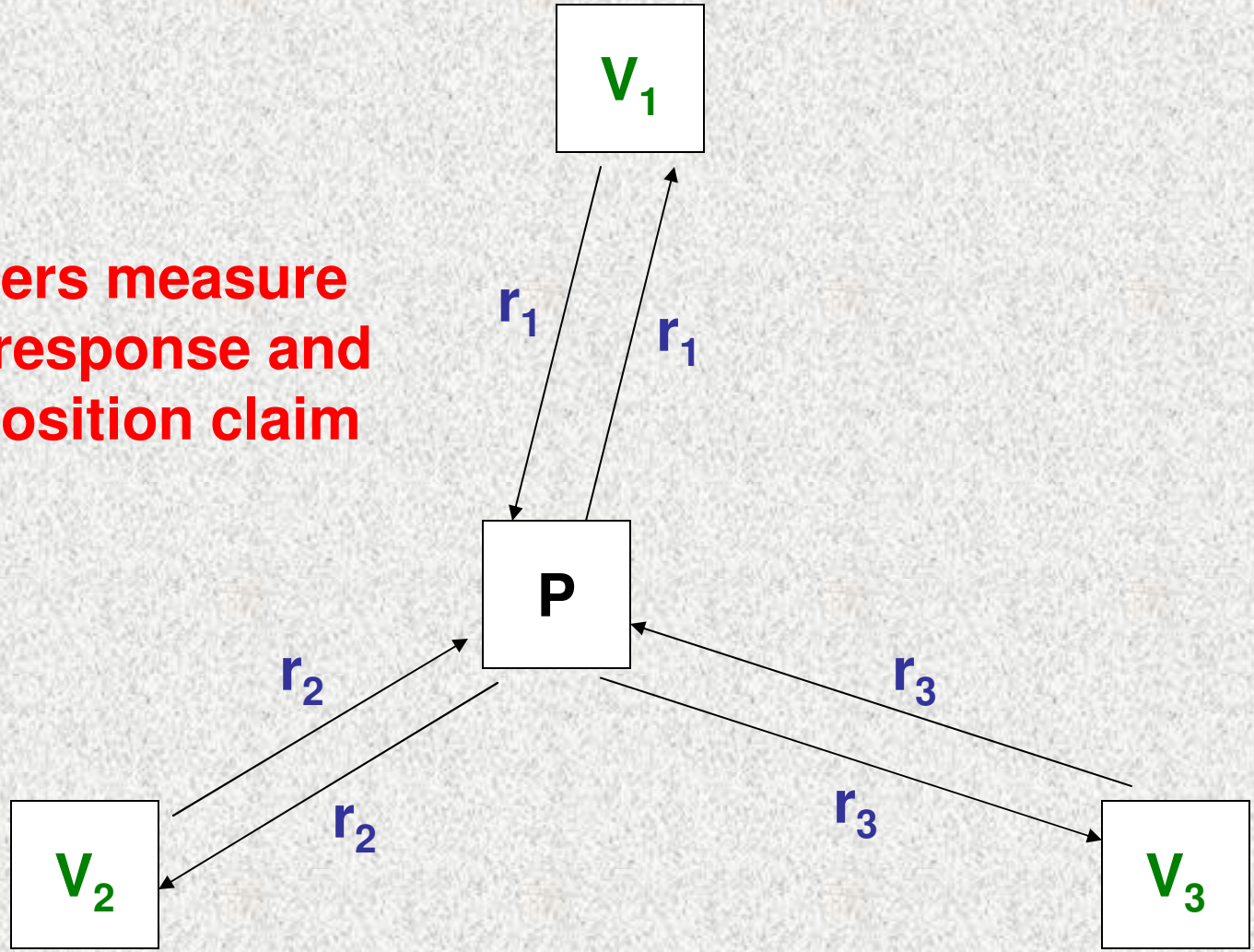


Time of response

Prover cannot claim to be closer to the verifier than he actually is

Triangulation [CH05]

3 Verifiers measure Time of response and verify position claim

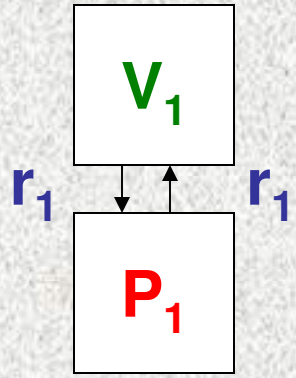


Triangulation [CH05]

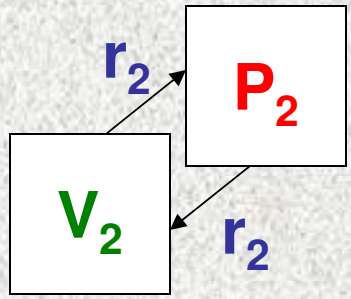
Attack with multiple colluding verifiers

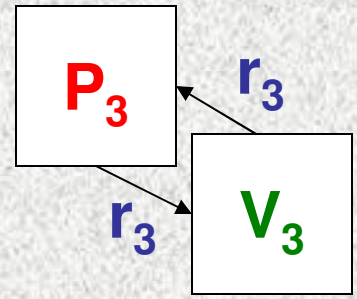
Works, but assumes a **single** adversary

P_i can delay response to V_i as if it were coming from P



Position P



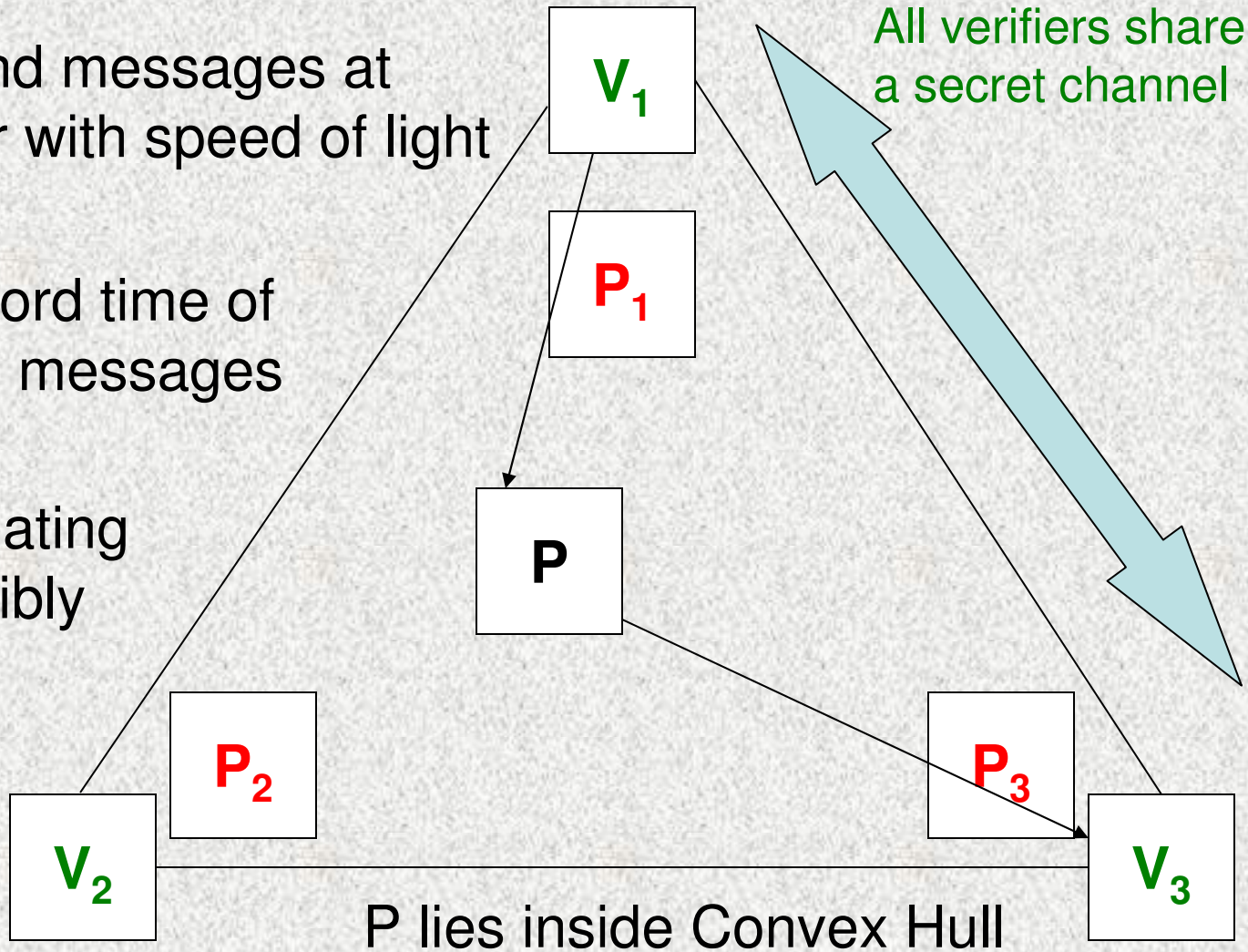


Talk Outline

- Vanilla Model
- Secure Positioning
  - Impossible in vanilla model
  - Positive information-theoretic results in the Bounded Retrieval Model
- Position-based Key Exchange
  - Positive information-theoretic results in the BRM

Vanilla Model

- Verifiers can send messages at any time to prover with speed of light
- Verifiers can record time of sent and received messages
- Multiple, coordinating adversaries, possibly computationally bounded

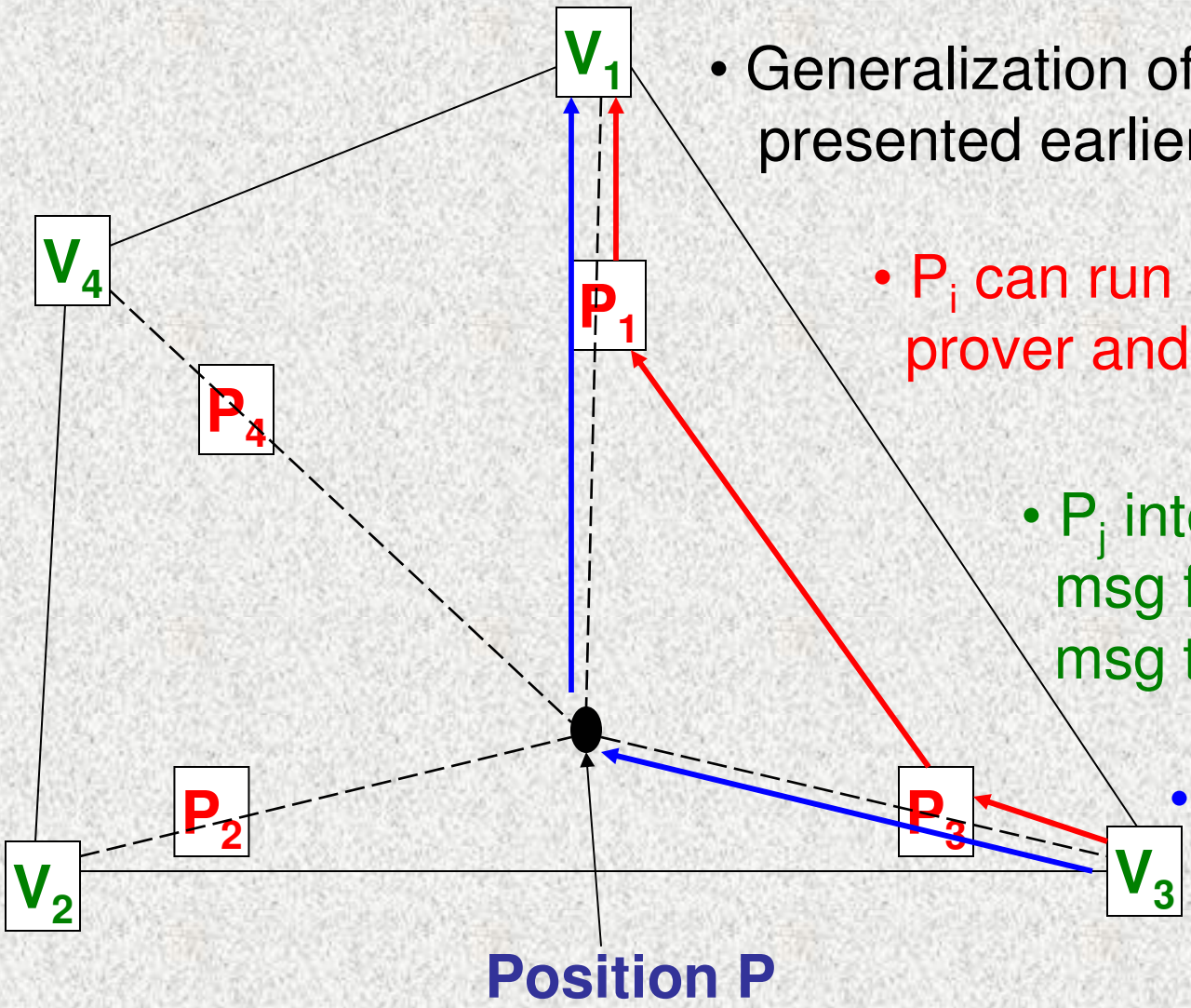


Lower Bound

Theorem: *There does not exist any protocol to achieve secure positioning in the Vanilla model*

Corollary: *Position-based key exchange is impossible in the Vanilla model*

Lower Bound – Proof sketch



- Generalization of attack presented earlier
- P_i can run exact copy of prover and respond to V_i
- P_j internally delays every msg from V_j and sends msg to P_i
- Blue path not shorter than red path

Lower bound implications

- Secure positioning and hence position-based cryptography is impossible in Vanilla model (even with computational assumptions!)
- Search for alternate models where position-based cryptography is possible?

CONSTRUCTIONS & PROOFS

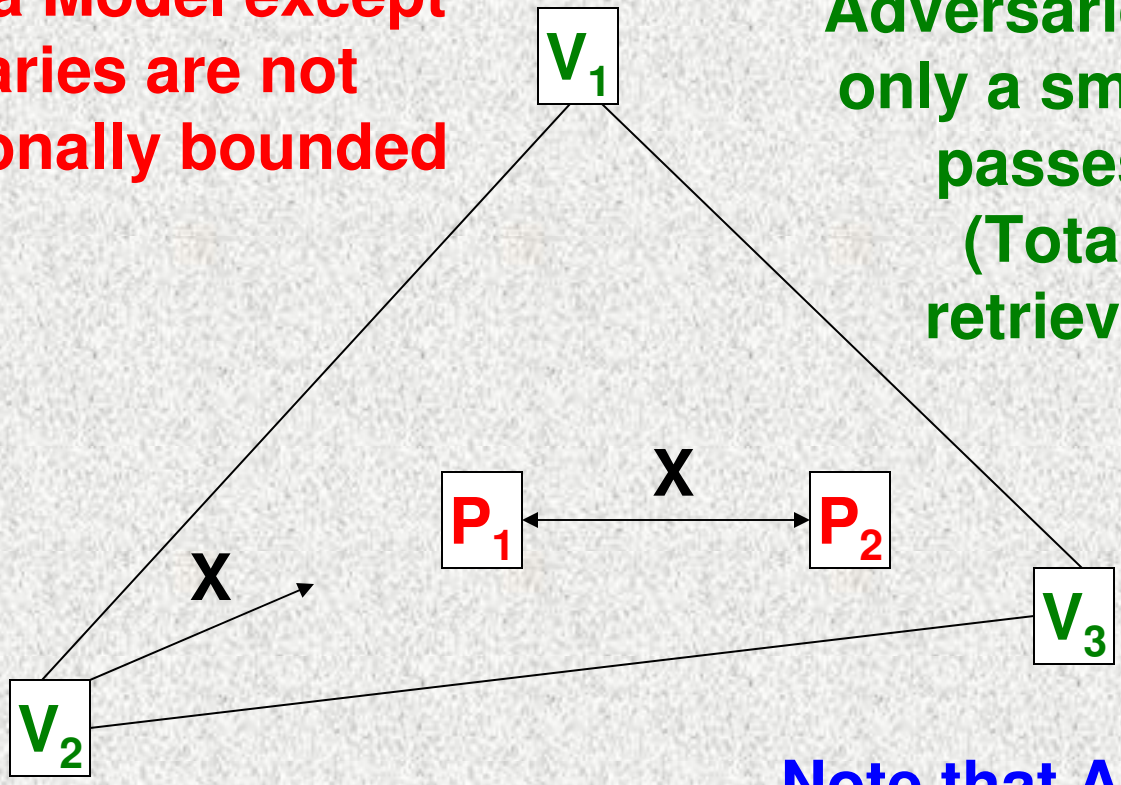
Bounded Retrieval Model (BRM) [Maurer'92, Dziembowski06, CLW06]

- Assumes long string X (of length n and high min-entropy) in the sky or generated by some party
- Assumes all parties (including honest) have retrieval bound βn for some $0<\beta<1$
- Adversaries can retrieve any information from X as long as the total information retrieved is bounded
- Several works have studied the model in great detail

BRM in the context of Position-based Cryptography

Like Vanilla Model except Adversaries are not computationally bounded

Adversaries can store only a small f(X) as X passes by…i.e. (Total |f(X)| < retrieval bound)



Verifiers can broadcast HUGE X

Note that Adversaries can NOT "reflect" X (violates BRM framework)

To make things more clear

- **Computation is instantaneous – modern GPS perform computation while using speed of light assumption**
  (relaxation → error in position)

- **Huge X travels in its entirety when broadcast and not as a stream**
  (again, relaxation → error in position)

Physically realizing BRM

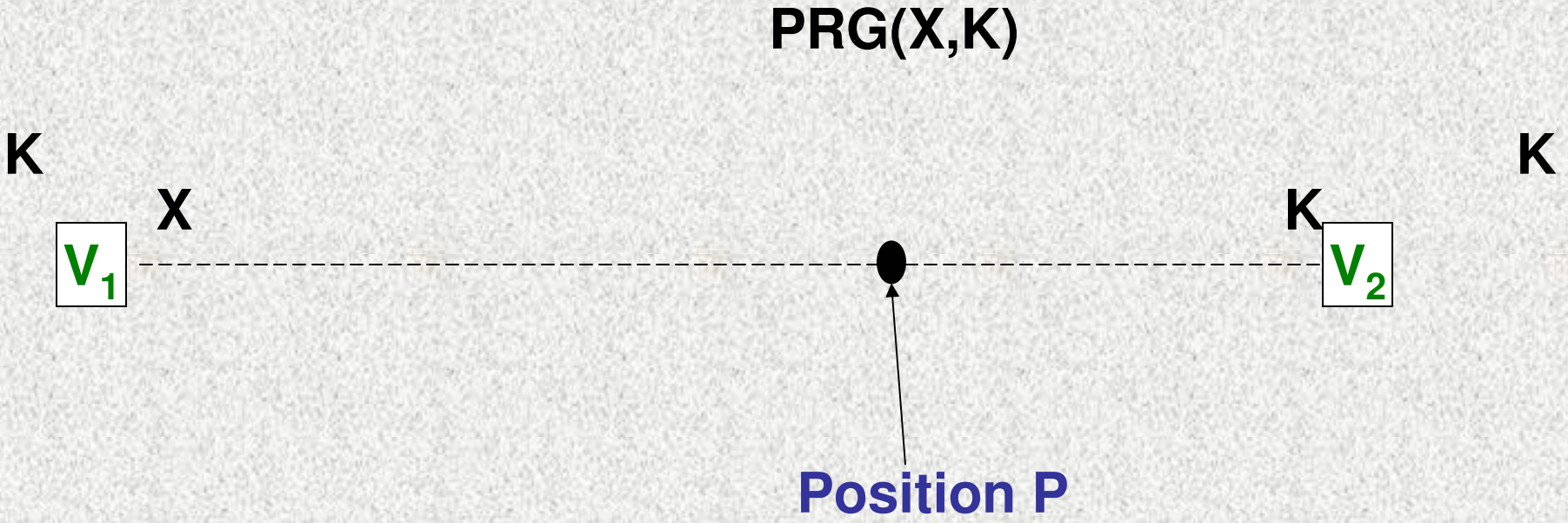
- Seems reasonable that an adversary can only retrieve small amount of information as a string passes by

- Verifiers could split X and broadcast the portions on different frequencies.
- Adversary cannot listen on all frequencies

BSM/BRM primitives needed

- Locally computable PRG from [Vad04]
- PRG takes as input string X with high min-entropy and short seed K
- PRG(X,K) ≈ Uniform, even given K and A(X) for arbitrary bounded output length function A

Secure Positioning in 1-Dimensional Space



V_1 measures time of response

and accepts if response is correct and received at the right time

Correctness of protocol follows from

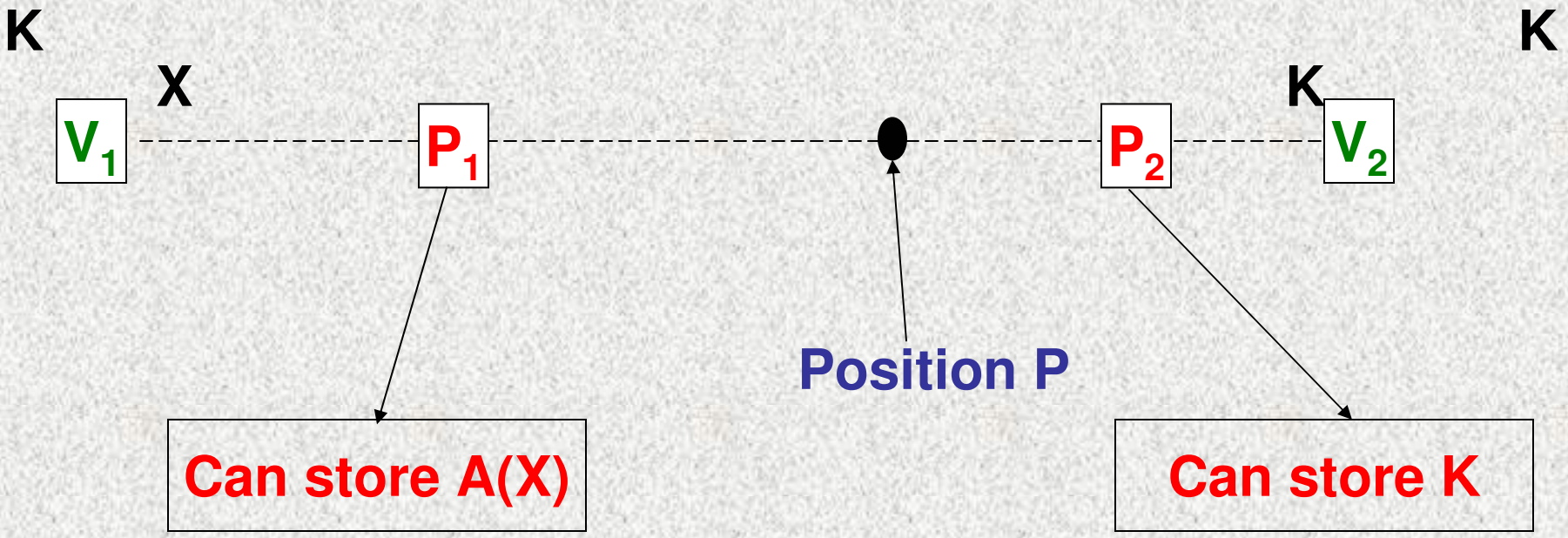
1. Prover at P can compute PRG(X,K)

2. V_1 can compute PRG(X,K) when broadcasting X

3. Response of prover from P will be on time

Secure Positioning in 1-Dimensional Space

Proof Intuition



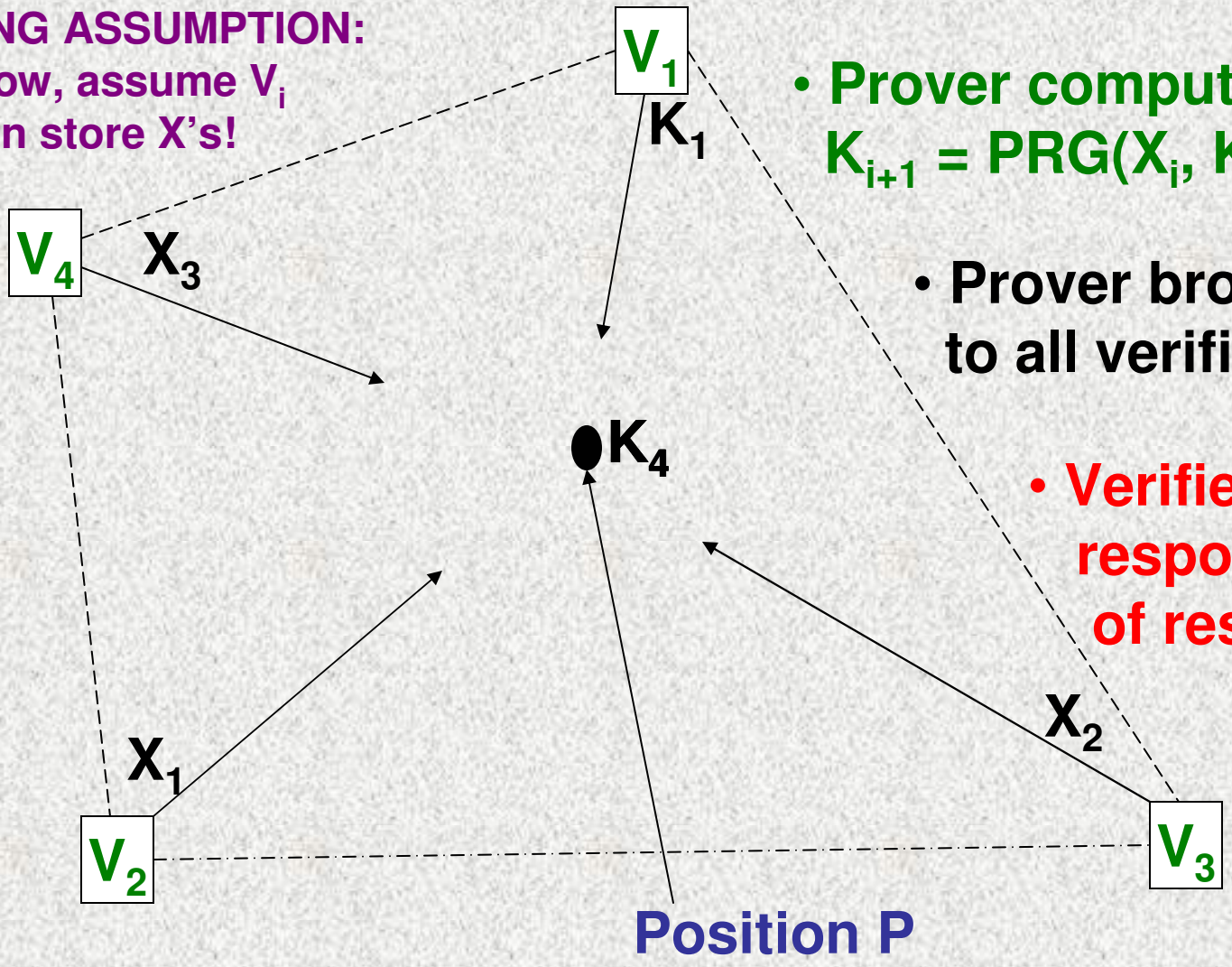
- P_1 closer to V_1 than P, but has only A(X) and K
- P_2 can compute PRG(X,K), but farther away from V_1 than P

Secure Positioning in 3-Dimensional Space

- First, we will make an UNREASONABLE assumption…
- Then show how to get rid of it!

Secure Positioning in 3-Dimensional Space

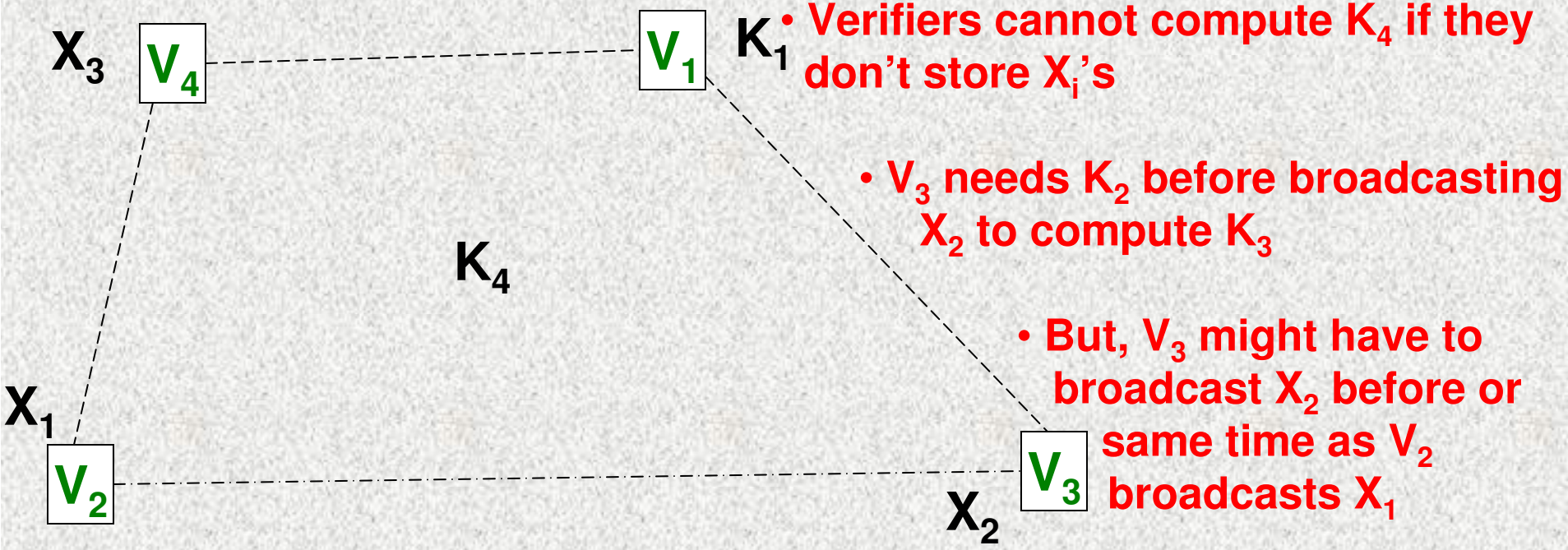
CHEATING ASSUMPTION:
For now, assume V_i can store X's!



- **Prover computes $K_{i+1} = PRG(X_i, K_i)$, $1 \le i \le 3$**
- **Prover broadcasts K_4 to all verifiers**
- **Verifiers check response & time of response**

Secure Positioning in 3-Dimensional Space

- Security will follow from security of position based based key exchange protocol presented later
- What about correctness??



- Verifiers cannot compute K_4 if they don't store X_i's
- V_3 needs K_2 before broadcasting X_2 to compute K_3
- But, V_3 might have to broadcast X_2 before or same time as V_2 broadcasts X_1

Secure Positioning in 3-Dimensional Space

ELIMINATING CHEATING:
Protocol when Verifiers cannot store X_i's

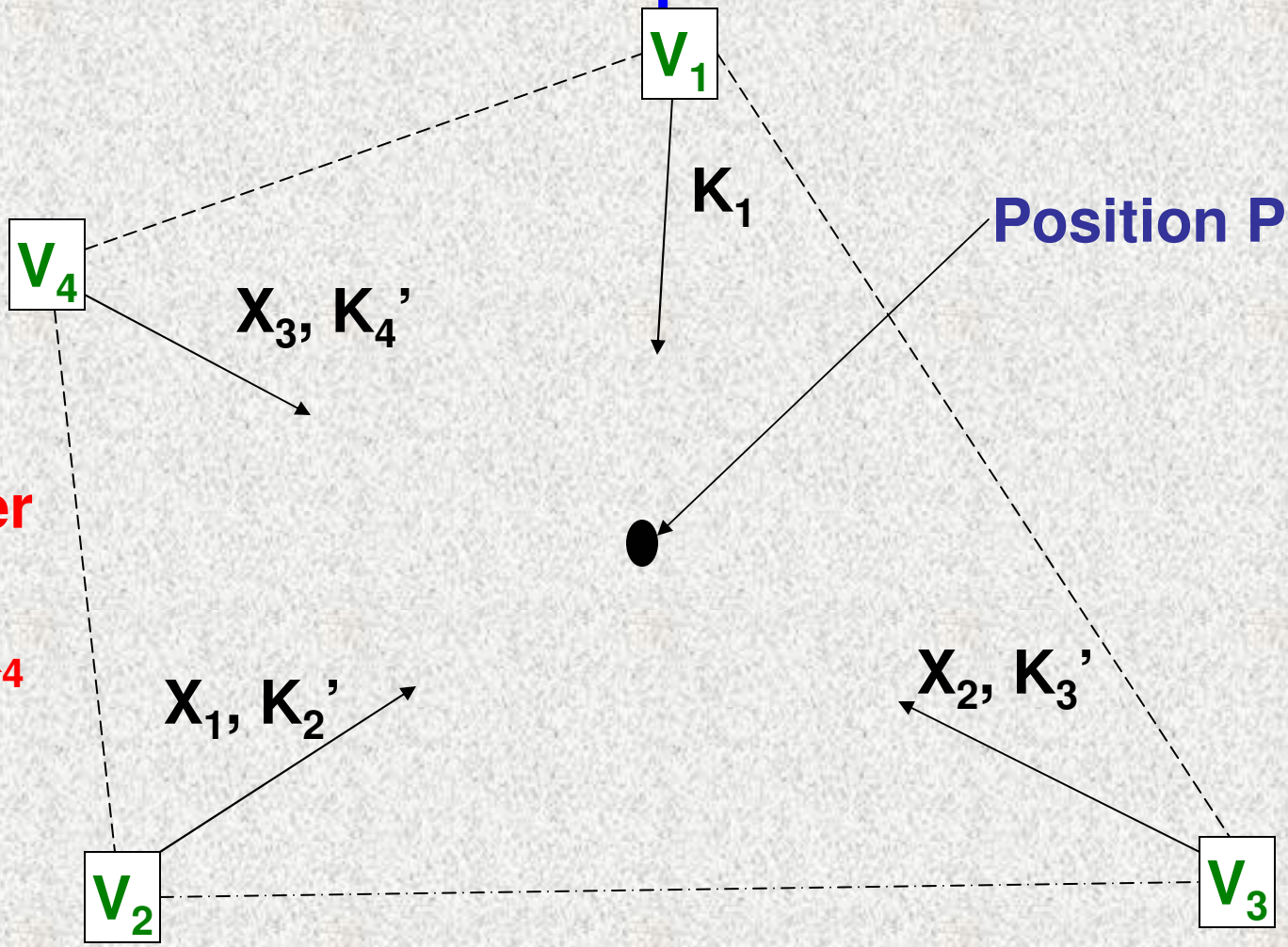
- V_1, V_2, V_3, V_4 pick K_1, K_2, K_3, K_4 at random before protocol

- Now, Verifiers know K_4; they must help prover compute it

- V_1 broadcasts K_1
- V_2 broadcasts X_1 and $K_2' = PRG(X_1,K_1)$ xor K_2
- V_3 broadcasts X_2 and $K_3' = PRG(X_2,K_2)$ xor K_3
- V_4 broadcasts X_3 and $K_4' = PRG(X_3,K_3)$ xor K_4

Verifiers secret share K_is and broadcast one share according to X_is

Secure Positioning in 3-Dimensional Space



- Note that prover can compute K_4 and broadcast K_4

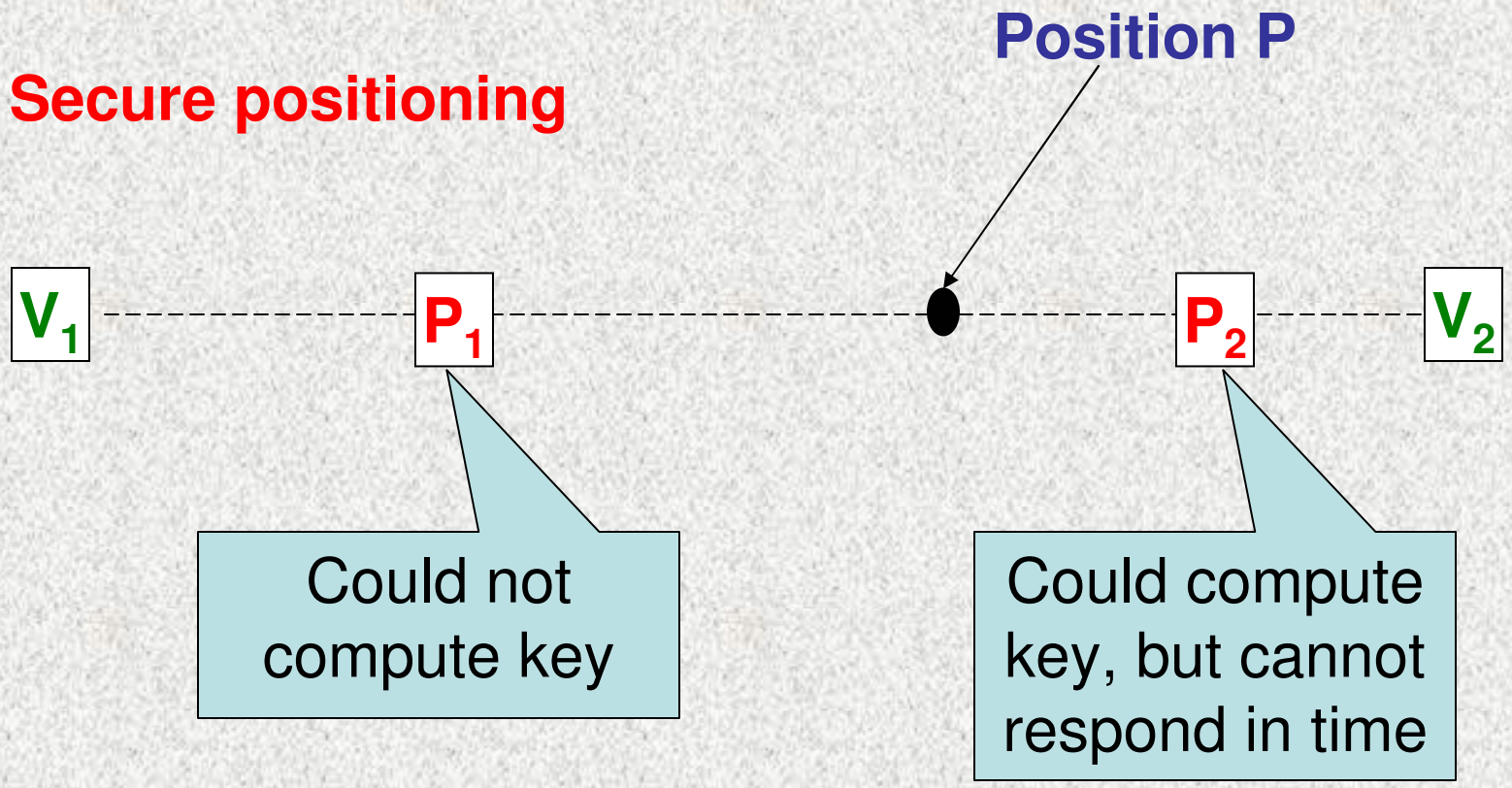
Secure Positioning: Bottom line

- We can do secure positioning in 3D in the bounded retrieval model
- We can obtain a protocol even if there is a small variance in delivery time when small positioning error is allowed

What else can we do in this model?

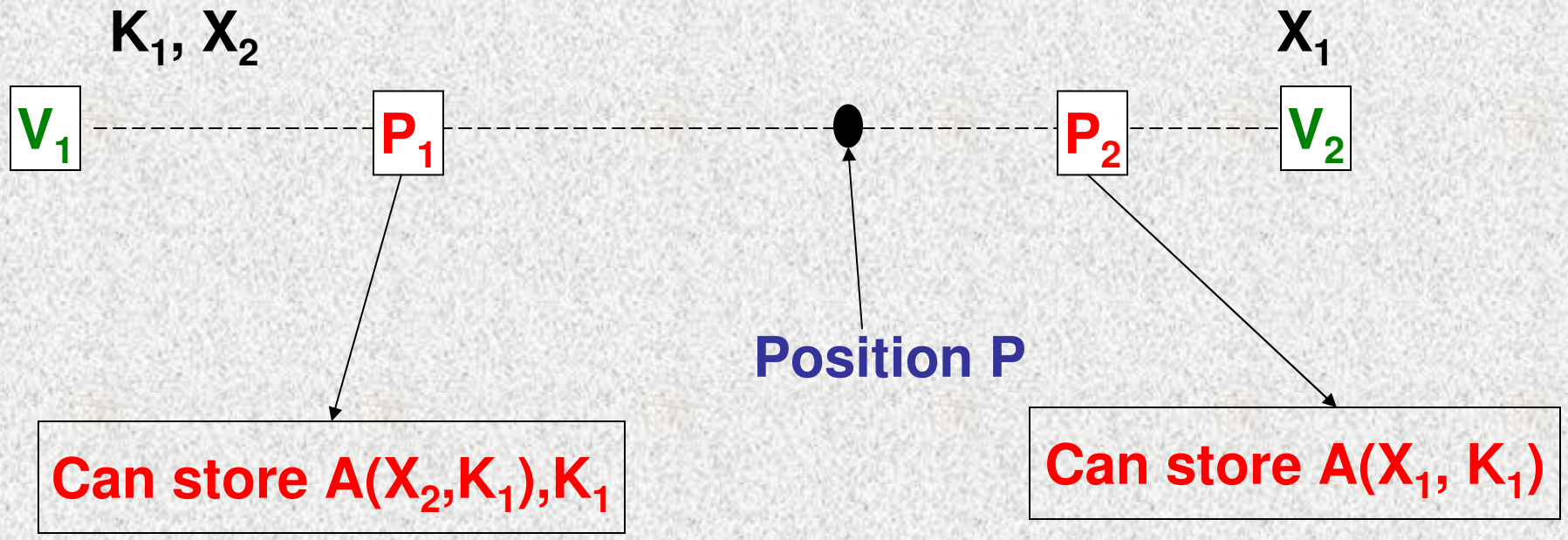
What about key agreement?

Information-theoretic Key Exchange in 1-Dimensional Space



Information-theoretic Key Exchange in 1-Dimensional Space

$K_3 = PRG(X_2, PRG(X_1, K_1))$



Seems like no adversary can compute $PRG(X_2, K_2)$

Intuition works!!

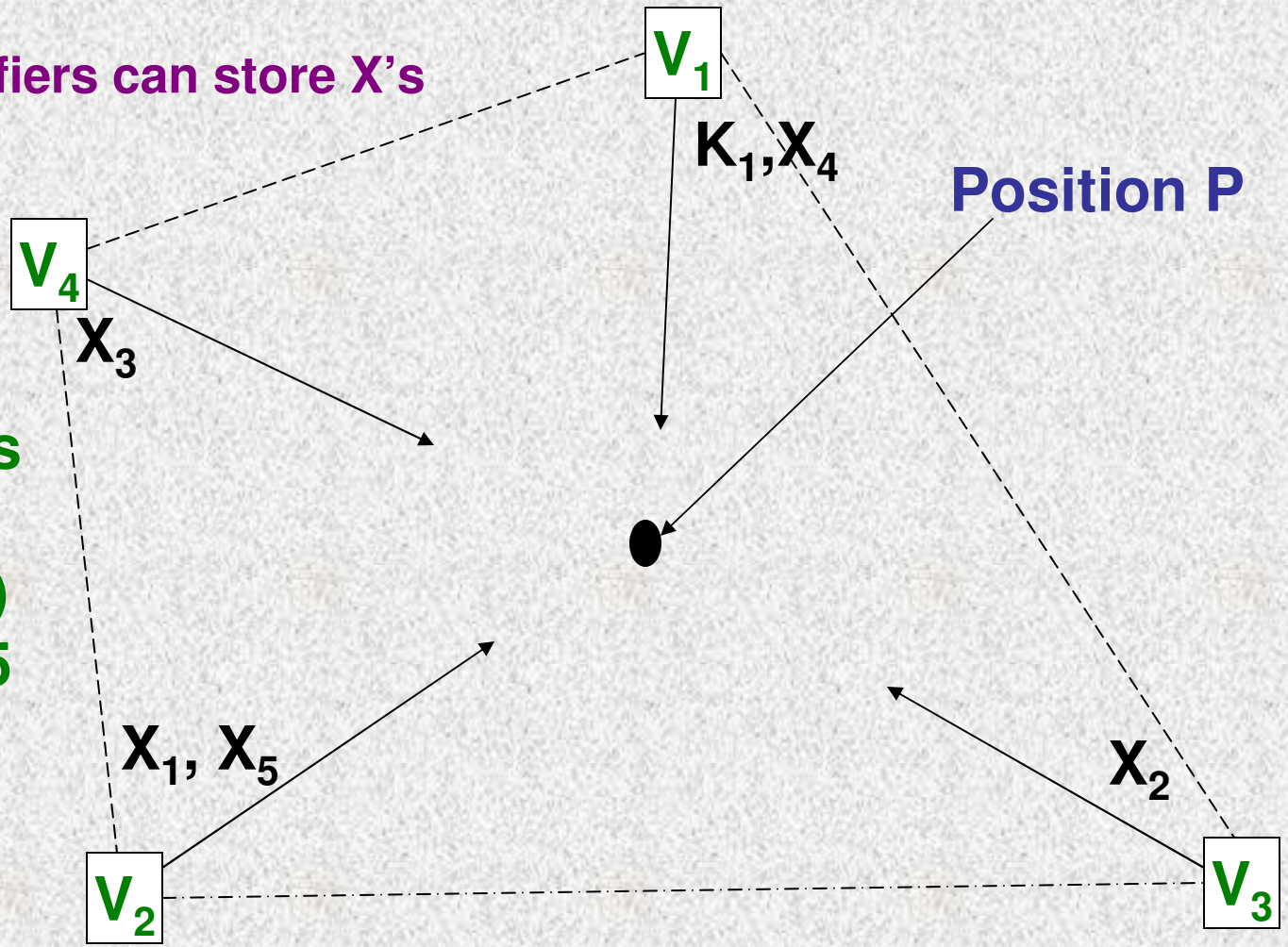
Information-theoretic Key Exchange in 3-Dimensional Space

Again assume Verifiers can store X's

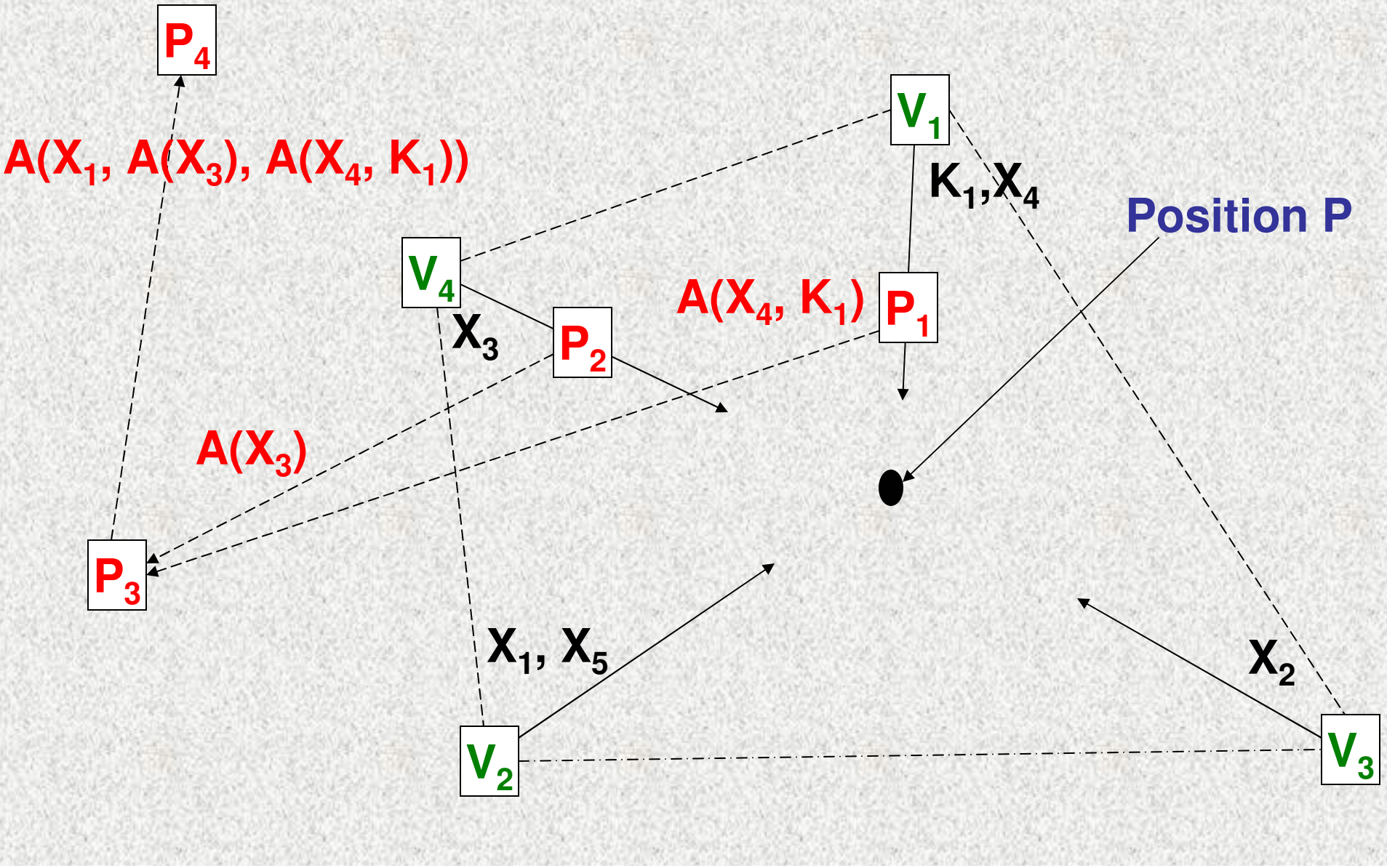
Prover computes

$K_{i+1} = PRG(X_i, K_i)$
$1 \le i \le 5$

K_6 is final key



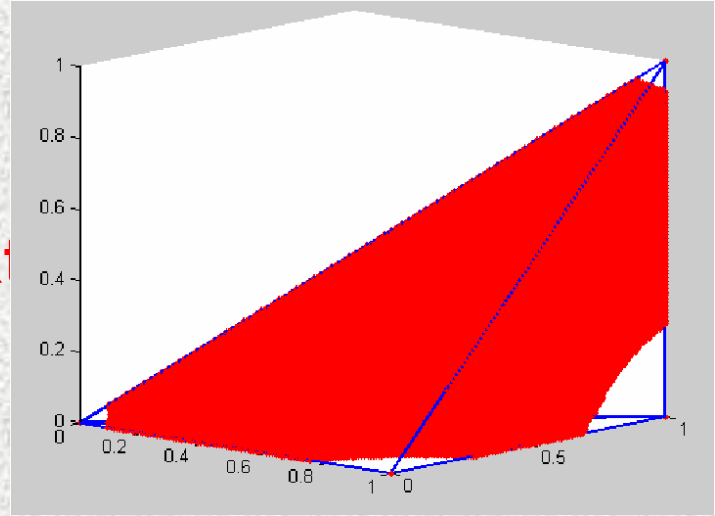
Subtleties in proof



Proof Ideas

Part 1: Geometric Arguments

- **A lemma ruling out any adversary simultaneously receiving all messages of the verifiers**
  - **Characterizes regions within convex hull where position-based key exchange is possible**
- **Combination of … o characterize information tha… t positions can obtain**



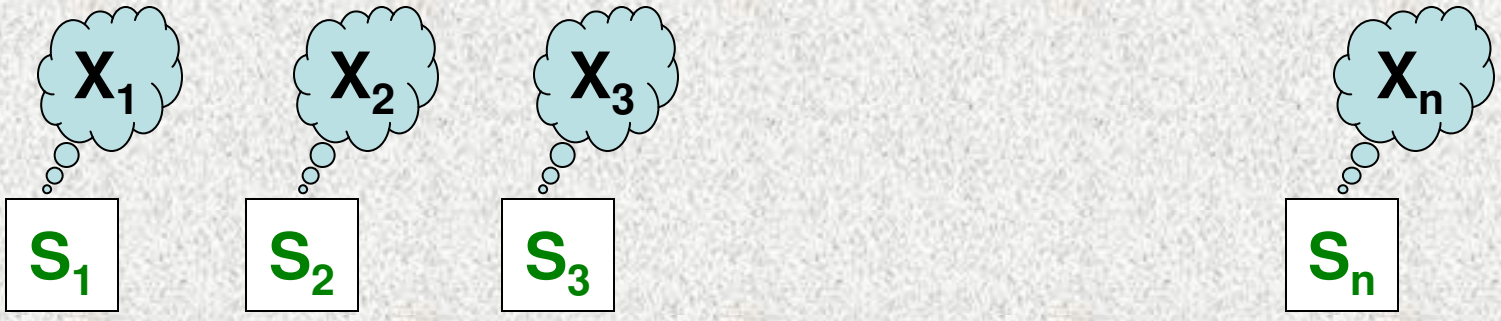
Proof Ideas

Part 2: Extractor Arguments

- **Build on techniques from Intrusion-Resilient Random Secret Sharing scheme of Dziembowski-Pietrzak [DP07]**

- **Show a reduction of the security of our protocol to a (slight) generalization of [DP07] allowing multiple adversaries working in parallel**

A REMINDER: Intrusion-Resilient Random Secret Sharing Scheme (IRRSS) [DP07]



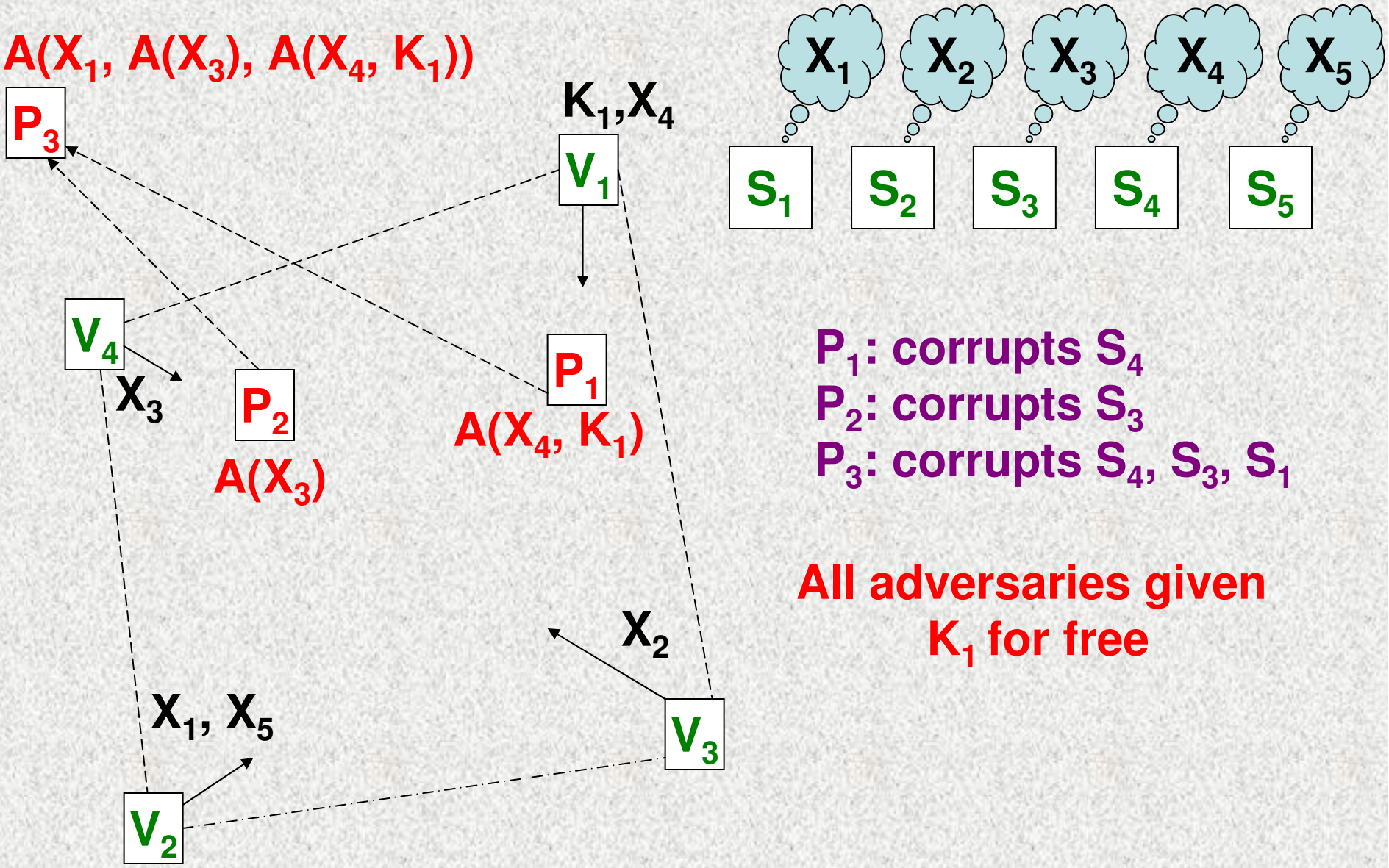
- K_1 is chosen at random and given to S_1
- S_i computes $K_{i+1} = PRG(X_i, K_i)$ and sends K_{i+1} to S_{i+1}
- S_n outputs key K_{n+1}

Bounded adversary can corrupt a sequence of players (with repetition) as long as sequence is valid

Valid sequence does not contain $S_1,S_2,..,S_n$ as a subsequence
Eg: If n = 5; 1342543412 5 is invalid, but 134525435 is valid

Then, K_{n+1} is statistically close to uniform

Reduction to IRRS



P_1: corrupts S_4
P_2: corrupts S_3
P_3: corrupts S_4, S_3, S_1

All adversaries given K_1 for free

Reduction to IRRS

- For every adversary A that receives information only from a verifier (not from other adversaries), we show a *corresponding* adversary B for [DP07] with valid corruption sequence C.

- If the *corresponding* adversary for A has an invalid corruption sequence in [DP07], then A must have received info from all verifiers simultaneously (Not possible by geometric lemma)

- Given two adversaries A_1 and A_2 with *corresponding* adversaries B_1 and B_2 (in [DP07]) and sequences C_1 and C_2, show how to get *corresponding* adversary B for $A_1 \cup A_2$ with corruption sequence C.

Conclusions

- WE HAVE SHOWN IN THE PAPER:
  - Position based Key Exchange in BRM for entire convex hull region (but computational security)
  - Protocol for position based Public Key Infrastructure
  - Protocol for position based MPC
- OPEN:
  - Other models?
    (Quantum: [C–Fehr–Goyal–Ostrovsky'09])
  - Other applications of position-based crypto?

Thank you

Full version available at

http://eprint.iacr.org/2009/364