Cryptography or Ramsey theory? The cool or the beautiful

Boaz Tsaban

Bar-Ilan University & Weizmann Institute of Science

27 Jul 08 CE

Topic I: Public Key Crypto (The cool)

Key Agreement Protocols

Key Agreement Protocols

Alice and Bob wish to communicate over an insecure channel.

Key Agreement Protocols

Alice and Bob wish to communicate over an insecure channel.

Diffie-Hellman (1976). Key Agreement Protocol: The most important breakthrough in cryptography.

Key Agreement Protocols

Alice and Bob wish to communicate over an insecure channel.

Diffie-Hellman (1976). Key Agreement Protocol: The most important breakthrough in cryptography.

Similar: Rivest-Shamir-Adleman (RSA, 1978).

Key Agreement Protocols

Alice and Bob wish to communicate over an insecure channel.

Diffie-Hellman (1976). Key Agreement Protocol: The most important breakthrough in cryptography.

Similar: Rivest-Shamir-Adleman (RSA, 1978).

Both use computations over commutative groups;
no long-term security; breakable by Quantum Computers.

Key Agreement Protocols

Alice and Bob wish to communicate over an insecure channel.

Diffie-Hellman (1976). Key Agreement Protocol: The most important breakthrough in cryptography.

Similar: Rivest-Shamir-Adleman (RSA, 1978).

Both use computations over commutative groups;
no long-term security; breakable by Quantum Computers.

No alternative (yet).

Key Agreement Protocols

Alice and Bob wish to communicate over an insecure channel.

Diffie-Hellman (1976). Key Agreement Protocol: The most important breakthrough in cryptography.

Similar: Rivest-Shamir-Adleman (RSA, 1978).

Both use computations over commutative groups;
no long-term security; breakable by Quantum Computers.

No alternative (yet).

Potential source: Combinatorial group theory
(noncommutative groups).

Key Agreement Protocols

Alice and Bob wish to communicate over an insecure channel.

Diffie-Hellman (1976). Key Agreement Protocol: The most important breakthrough in cryptography.

Similar: Rivest-Shamir-Adleman (RSA, 1978).

Both use computations over commutative groups;
no long-term security; breakable by Quantum Computers.

No alternative (yet).

Potential source: Combinatorial group theory
(noncommutative groups).

WIN/WIN: Better KAP / Efficient algorithms.

Diffie-Hellman KAP

Diffie-Hellman KAP

Public: Prime p; generator g of $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$.

Diffie-Hellman KAP

Public: Prime p; generator g of $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$.

Alice chooses $a \in \{1, \ldots, p-1\}$; sends g^a to Bob.

Diffie-Hellman KAP

Public: Prime p; generator g of $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$.

Alice chooses $a \in \{1, \ldots, p-1\}$; sends g^a to Bob.

Bob chooses $b \in \{1, \ldots, p-1\}$; sends g^b to Alice.

Diffie-Hellman KAP

Public: Prime p; generator g of $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$.

Alice chooses $a \in \{1, \ldots, p-1\}$; sends g^a to Bob.

Bob chooses $b \in \{1, \ldots, p-1\}$; sends g^b to Alice.

Shared key:

$$\text{(Alice)} \quad (g^b)^a = g^{ba} = g^{ab} = (g^a)^b \quad \text{(Bob)}$$

Diffie-Hellman KAP

Public: Prime p; generator g of $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$.

Alice chooses $a \in \{1, \ldots, p-1\}$; sends g^a to Bob.

Bob chooses $b \in \{1, \ldots, p-1\}$; sends g^b to Alice.

Shared key:

$$\text{(Alice)} \quad (g^b)^a = g^{ba} = g^{ab} = (g^a)^b \quad \text{(Bob)}$$

There are similar algorithms in the noncommutative case.

Suggested Project I

Suggested Project I

Optimize algorithms for operations in noncommutative groups.

Suggested Project I

Optimize algorithms for operations in noncommutative groups.

Learn and use cutting-edge software and C/C++ libraries to attack the underlying mathematical problems.

Suggested Project I

Optimize algorithms for operations in noncommutative groups.

Learn and use cutting-edge software and C/C++ libraries to attack the underlying mathematical problems.

Requirements:

1. Top student.
2. Loves programming and optimizing ("hacker").

Topic II: Ramsey theory (The beautiful)

The Ramsey Phenomenon

The Ramsey Phenomenon

If a rich object is partitioned into few pieces,

The Ramsey Phenomenon

If a rich object is partitioned into few pieces,
at least one piece must be rich.

The Ramsey Phenomenon

If a rich object is partitioned into few pieces,
at least one piece must be rich.

Pigeonhole principle. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 ...

The Ramsey Phenomenon

If a rich object is partitioned into few pieces,
at least one piece must be rich.

Pigeonhole principle. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 ...

The Ramsey Phenomenon

If a rich object is partitioned into few pieces,
at least one piece must be rich.

Pigeonhole principle. 1 4 5 7 9 11 14 . . .

The Ramsey Phenomenon

If a rich object is partitioned into few pieces,
at least one piece must be rich.

Pigeonhole principle. 1 4 5 7 9 11 14 ...

van der Waerden Theorem. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 ...

The Ramsey Phenomenon

If a rich object is partitioned into few pieces,
at least one piece must be rich.

Pigeonhole principle. 1 4 5 7 9 11 14 ...

van der Waerden Theorem. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 ...

The Ramsey Phenomenon

If a rich object is partitioned into few pieces,
at least one piece must be rich.

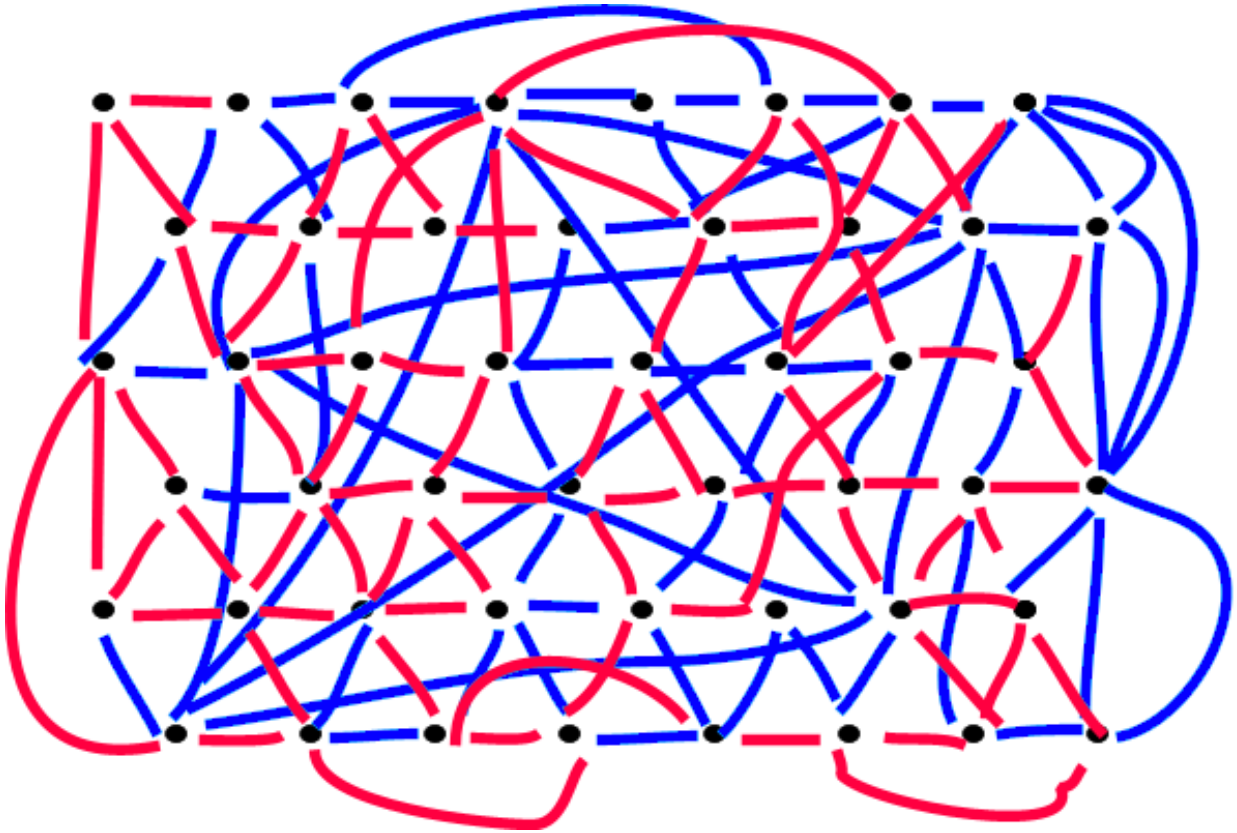
Pigeonhole principle. 1 4 5 7 9 11 14 ...

van der Waerden Theorem. 1 4 5 7 9 11 14 ...

Ramsey's Theorem

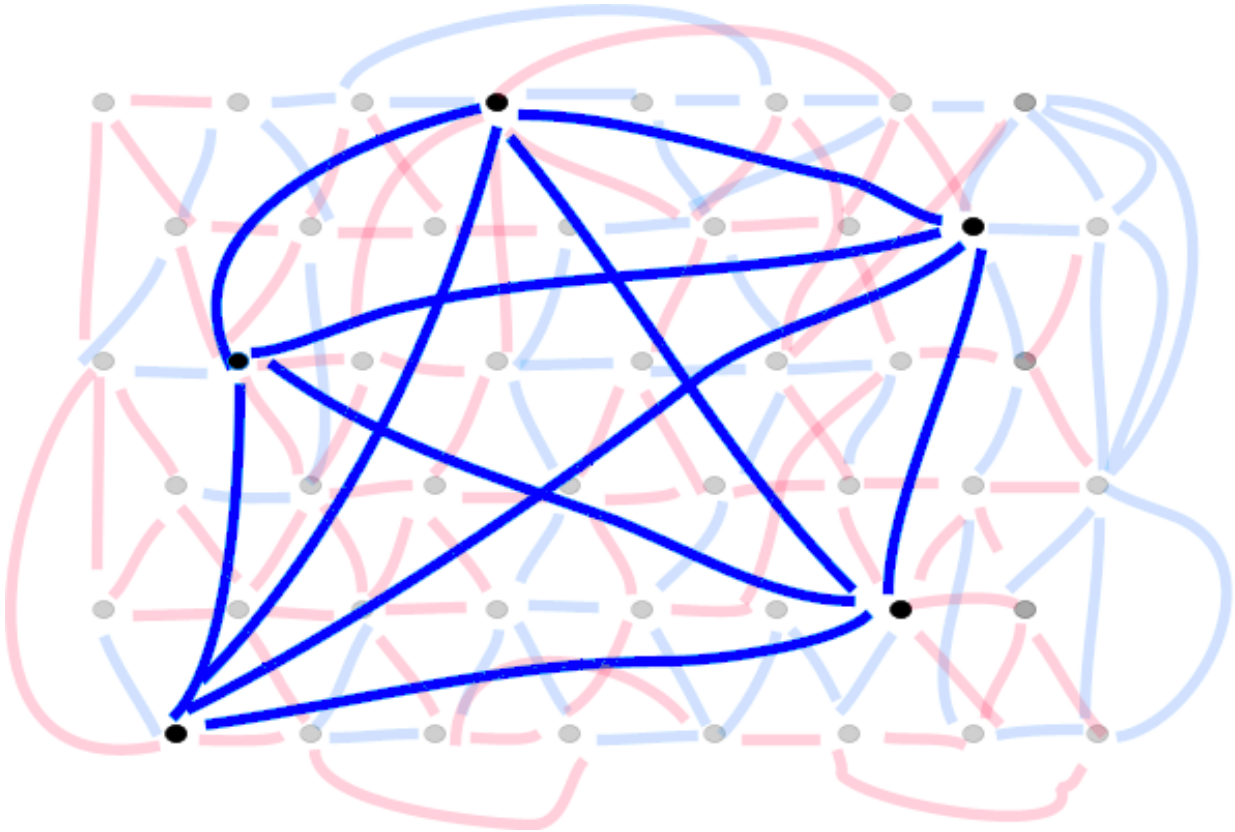
Ramsey's Theorem

If the edges of an infinite complete graph have two colors



Ramsey's Theorem

If the edges of an infinite complete graph have two colors



Then $\exists$ infinite complete monochromatic subgraph.

Suggested Project II

Suggested Project II

Study a very new approach and apply it.

Suggested Project II

Study a very new approach and apply it.

Requirements:

1. Top student.
2. Loves beautiful mathematics.