Elliptic Curves, Cryptography and Computation

Victor S. Miller

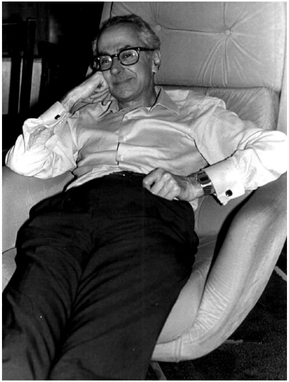
IDA Center for Communications Research
Princeton, NJ 08540 USA

18 Oct, 2010

"All my gadgets are old. I'd like some new gadgets."

Serge Lang

It is possible to write endlessly about Elliptic Curves – this is not a threat!



Solutions to Diophantine Equations

A lot of research in Mathematics has been motivated by hard, but easy to state problems.
Famous example:

Fermat's Last Theorem

$x^n + y^n = z^n$.

Computation versus Existence

Proving that something exists versus computing it efficiently.
With the availability of great computing resources, the quest for computing mathematical objects, so prominent in the 19th century, has been revived.

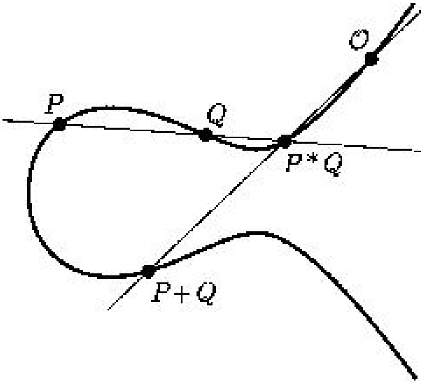
A field that's becoming more known

- Studied intensively by number theorists for past 100 years.
- Until recently fairly arcane.
- Before 1985 – virtually unheard of in crypto and theoretical computer science community.
- In mathematical community: Mathematical Reviews has about 200 papers with "elliptic curve" in the title before 1984, but in all now has about 2000.
- A google search yield 83 pages of hits for the phrase "elliptic curve cryptography".

Elliptic Curves

- Set of solutions (points) to an equation $E : y^2 = x^3 + ax + b$.
- More generally any cubic curve – above is "Weierstrass Form".
- The set has a natural geometric group law, which also respects field of definition – works over finite fields.
- Weierstrass $\mathfrak{p}$ function: $\mathfrak{p}'^2 = 4\mathfrak{p}^3 - g_2\mathfrak{p} - g_3$.
- Only doubly-periodic complex function.

Chord and Tangent Process



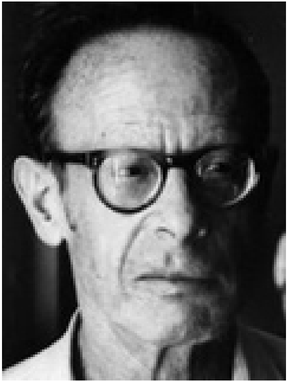
Abelian Varieties

- Multi-dimensional generalization of elliptic curves.
- Dimension g has $2g$ periods.
- Also has group law, which respects field of definition.
- First studied by Abel (group is also abelian – a happy conincidence!).

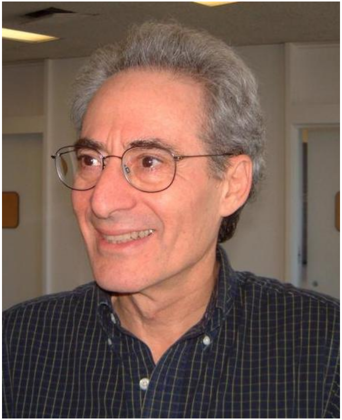
Elliptic Curves over Rational Numbers

- Set of solutions always forms a finitely generated group – Mordell-Weil Theorem.
- There is a procedure to find generators – very often quite efficient (but not even known to terminate in many cases!).
- Size function – "Weil height" – roughly measures number of bits in a point.
- Tate height – smoothing of height. Points form a lattice.

Louis Mordell, André Weil



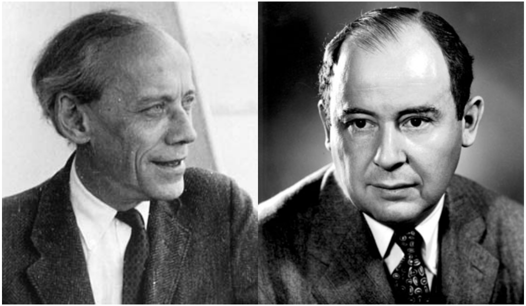
Barry Mazur



No point on an elliptic curve over $\mathbb{Q}$ has order more than 12.

John Tate

Emil Artin and John von Neumann

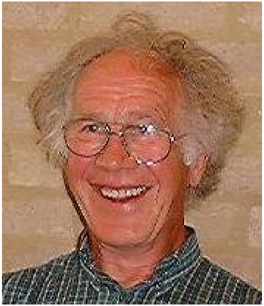


In 1952 Emil Artin asked John von Neumann to do a calculation on the ENIAC computer about cubic Gauss sums related to the distribution of the number of points on $y^2 = x^3 + 1 \bmod p$.

Bryan Birch and Peter Swinnerton-Dyer

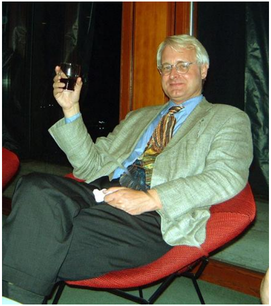
Birch and Swinnerton-Dyer formulated their important conjecture only after extensive computer calculations.

Bryan Birch and Peter Swinnerton-Dyer



The state of Number Theory

Number Theory is a beautiful garden – Carl Ludwig Siegel



Oil was discovered in the garden. – Hendrik W. Lenstra, Jr.

Public Key

- In 1976 Diffie and Hellman proposed the first public key protocol.
- Let p be a large prime.
- Non zero elements of $\mathbb{F}_p$ form cyclic group, $g \in \mathbb{F}_p$ a "primitive root" – a generator.
- Security dependent upon difficulty of solving:

  DHP: Given p, g, g^a and g^b, find g^{ab} (note a and b are not *known.*

- Speculated: only good way to solve DHP is to solve:

  DLP: Given p, g, g^a, find a.

- Soon generalized to work over any finite field – especially $\mathbb{F}_{2^n}$.

Marty Hellman and Whit Diffie

Whit Diffie and Marty Hellman

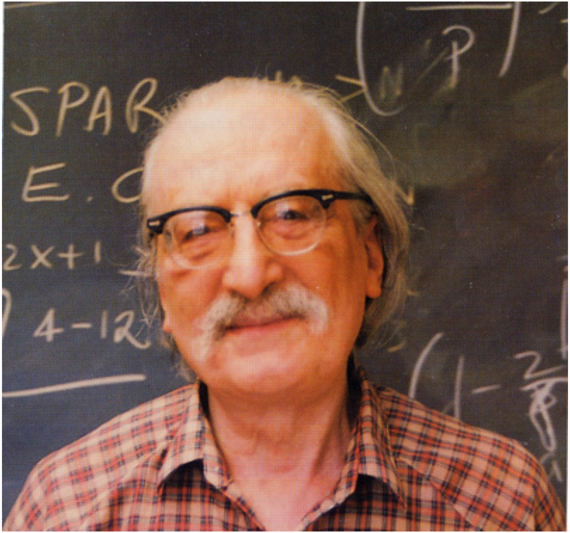

Attacks on DLP

- Pohlig-Hellman – only need to solve problem in a cyclic group of prime order – security depends on largest prime divisor q of $p-1$ (or of $2^n - 1$ for $\mathbb{F}_{2^n}$).
- Shanks "baby step giant step" in time $O(\sqrt{q})$. They speculated that this was the best one could do.
- A. E. Western, J. C. P. Miller in 1965, Len Adleman in 1978 – heuristic algorithm in time

$$O(\exp(\sqrt{2 \log p \log \log p})).$$

- Hellman and Reynieri – similar for $\mathbb{F}_{2^n}$ with 2^n replacing p in above.
- Fuji-Hara, Blake, Mullin, Vanstone – a significant speed up of Hellman and Reynieri.

Dan Shanks



Len Adleman

My initiation into serious cryptography

- Friend and colleague of Don Coppersmith since graduate school.
- In 1983 Fuji-Hara gave talk at IBM, T. J. Watson Research Center "How to rob a bank", on work with Blake, Mullin and Vanstone.
- The Federal Reserve Bank of California wanted to use *DL* over $\mathbb{F}_{2^{127}}$ to secure sensitive transactions.
- Hewlett-Packard starting manufacturing chips to do the protocol.
- Fuji-Hara's talk piqued Don's interest.

Don Coppersmith

Ryoh Fuji-Hari, Ian Blake, Ron Mullin, Scott Vanstone




Factoring, Factor Bases and Discrete Logarithms

- Subexponential time factoring of integers.
- CFRAC: Morrison and Brillhart. Brillhart coined the term "Factor Base"
- Rich Schroeppel – Linear Sieve
- Carl Pomerance: coined the term "smooth", the "quadratic sieve" and the notation

$$L_x[a; b] := \exp(b(\log x)^a(\log\log x)^{1-a}).$$

- From analyzing probability that a random integer factors into small primes ("smooth").

John Brillhart

Rich Schroeppel

Carl Pomerance

Coppersmith's attack on DL over $\mathbb{F}_{2^{127}}$

- After Fuji-Hara's talk, Don started thinking seriously about the DL problem.
- We would talk a few times a week about it – this taught me a lot about the intricacies of the "index calculus" (coined by Odlyzko to describe the family of algorithms).
- The BFMV algorithm was still $L[1/2]$ (with a better constant in the exponential).
- Don devised an $L[1/3]$ algorithm for $\mathbb{F}_{2^n}$.
- Successfully attacked $\mathbb{F}_{2^{127}}$ in seconds.
- Ten years later Dan Gordon devised an $L[1/3]$ algorithm for $\mathbb{F}_p$.

Dan Gordon

Were Hellman and Pohlig right about discrete logarithms?

- Yes, and no.
- For original problem – no.
- Needed to use specific property ("smoothness") to make good attacks work.
- Nechaev (generalized by Shoup) showed that $O(\sqrt{q})$ was the best that you could do for "black box groups".
- What about DHP? Maurer, and later Boneh and Lipton gave strong evidence that it was no harder than DL (used elliptic curves!).

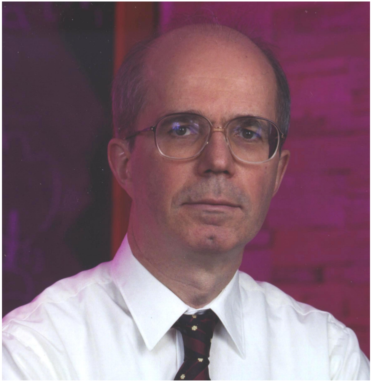
Victor Shoup

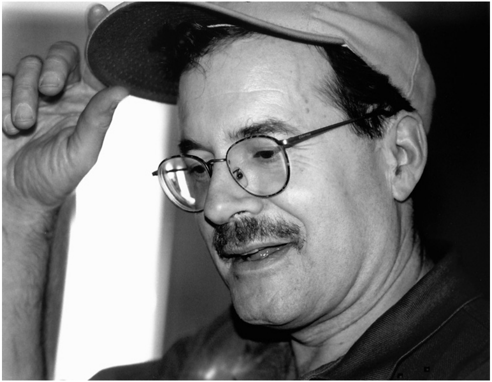
Ueli Maurer, Dan Boneh, Dick Lipton

A New Idea

- While I visted Andrew Odlyzko and Jeff Lagarias at Bell Labs in August 1983, they showed me a preprint of a paper by René Schoof giving a polynomial time algorithm for counting points on an elliptic curve over $\mathbb{F}_p$.
- Shortly thereafter I saw a paper by Hendrik Lenstra (Schoof's advisor) which used elliptic curves to factor integers in time $L[1/2]$.
- This, combined with Don's attack on DL over $\mathbb{F}_{2^n}$ got me to thinking of using elliptic curves for DL.

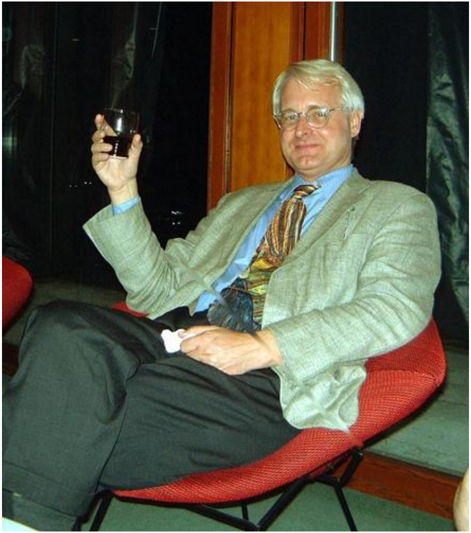
Andrew Odlyzko, Jeff Lagarias





Rene Schoof

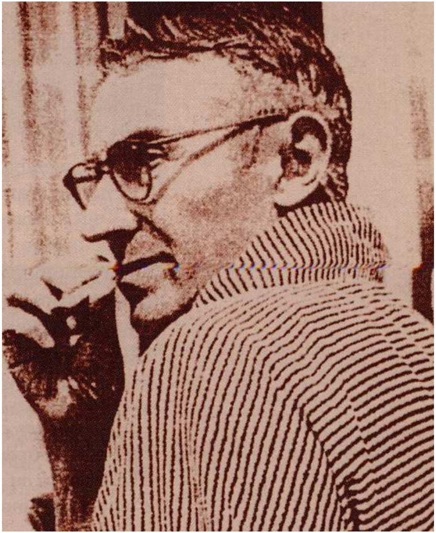
Hendrik W. Lenstra, Jr.



Diffie-Hellman in General Groups

- Many people realized that DH protocol only needed associative multiplication.
- Some other protocols needed inverse. So one can do it in a group.
- Why use another group?
- Finite fields (mostly) have index calculus attacks.
- Good candidate: algebraic groups – group law and membership given by polynomial or rational functions.
- Chevalley's Theorem: algebraic groups are extensions of matrix groups by abelian varieties (over finite fields).
- Pohlig and Hellman: DL "lives" in either matrix group or abelian variety.
- Using eigenvalues – matrix group DL reduces to multiplicative group DL in a small extension.

Claude Chevalley



Index Calculus

- Given primitive root g of a prime p. Denote by $x = \log_g(a)$, an integer in $[0, p-1]$ satisfying $g^x = a$.
- Choose a factor base $\mathcal{F} = \{p_1, \ldots, p_k\}$ first k primes.
- Preprocess: find $\log_g(p_i)$ for all $p_i \in \mathcal{F}$.
- Individual log: use the table $\log_g(p_i)$ to find $\log_g(a)$.

Some details: Preprocess

- Preprocess: Choose random $y \in \mathbb{F}_p$ calculate $z = g^y \pmod{p}$, and treat z as an integer.
- See if z factors into the prime in $\mathcal{F}$ only.
- If it does we have
$$z = p_1^{e_1} \dots p_k^{e_k}.$$
- Reduce $\bmod p$ and take logs:
$$y = e_1 \log_g(p_1) + \cdots + e_k \log_g(p_k).$$
- y and e_i are known: get linear equation in unknowns $\log_g(p_i)$.
- When we have enough equations, solve for unknowns.

Some details: Individual Logs

- Individual Logs: Choose random $y \in \mathbb{F}_p$ calculate $z = ag^y \pmod{p}$, and treat z as an integer.
- See if z factors into the prime in $\mathcal{F}$ only.
- If it does we have
$$z = p_1^{e_1} \dots p_k^{e_k}.$$
- Reduce $\bmod p$ and take logs:
$$\log_g(a) + y = e_1 \log_g(p_1) + \cdots + e_k \log_g(p_k).$$
- Using the values of $\log_g(p_i)$ computed previously this gives answer.
- Increasing k increases probability of success, but also increases size of linear algebra problem. Optimal value yields time $O(L_p[1/2; c])$ for some constant c.
- Coppersmith and Gordon (NFS) use clever choice to get probability of success up (plus a lot of difficult details).

Factor Base for Elliptic Curves?

- Given elliptic curve E over $\mathbb{F}_p$, find $\widetilde{E}$ over $\mathbb{Q}$ which reduces $\bmod p$ to E.
- Question: if $P \in E(\mathbb{F}_p)$ is random, how to find $\widetilde{P} \in \widetilde{E}(\mathbb{Q})$ which reduces to $P \bmod p$?
- Big qualitative difference – assuming various standard conjectures (especially one by Serge Lang), one can show that the fraction of points in $\widetilde{E}(\mathbb{Q})$ whose number of bits are polynomial in $\log p$ are $O((\log\log p)^c)$ for some c.
- Probability of succeeding in random guess is far too small.
- Other advantage of Elliptic Curves: there are lots of them over $\mathbb{F}_p$ of all different sizes $\approx p$ (also used by Lenstra in his factoring algorithm).

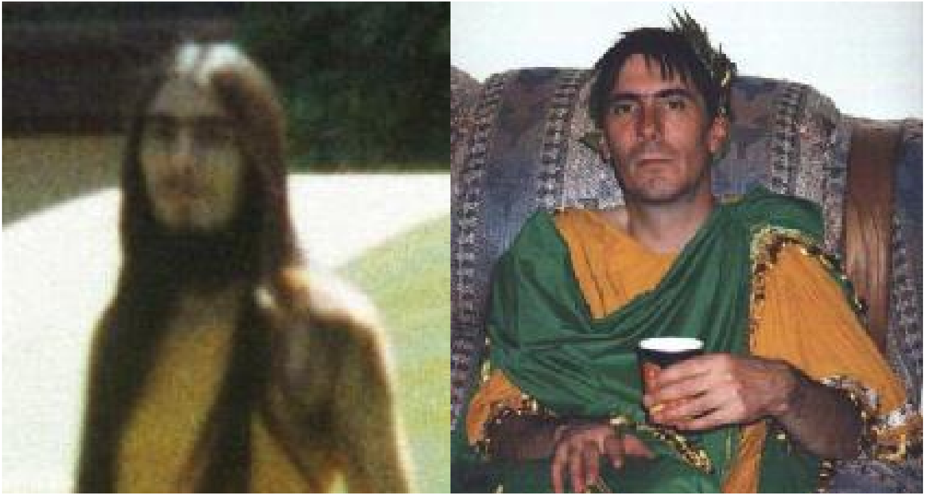
Crypto '85 and after

- I corresponded with Odlyzko while forming my ideas.
- The day that I finally convinced him, he reported receving a letter from Neal Koblitz (who was in Moscow) also proposing using Elliptic Curves for a Diffie-Hellman protocol.
- At Crypto: the talk immediately preceding mine was given by Nelson Stephens – an exposition of Lenstra's factoring method. The audience got a double dose of Elliptic Curves.
- After my talk, Len Adleman and Kevin McCurley asked that I give them an impromptu exposition about the theory of elliptic curves.
- The next year Len, and Ming-Deh Huang asked that I give them a similar talk about abelian varieties – lead to their random polynomial time algorithm for primality proving.
- Corresponded extensively with Burt Kaliski while he was working on his thesis about elliptic curves. He was first to implement my algorithm for the Weil pairing.

Neal Koblitz

Nelson Stephens

Kevin McCurley



Ming-Deh Huang

Burt Kaliski

A few weak cases

- Menezes, Okamoto and Vanstone, using Weil pairing (see below) in a case I missed – supersingular curves (more generally "low embedding degree").
- Later by Frey and Rück using the Tate Pairing for curves with $p - 1$ points.
- Nigel Smart, Igor Semaev, Takakazu Satoh and Kiyomichi Araki for curves with p points.

Alfred Menezes, Tatsuaki Okamoto, Scott Vanstone

Gerhard Frey, Hans-Georg Rück

Nigel Smart

Primality proving

- Goldwasser and Kilian – gave polynomial size certificate for primality form almost all primes using elliptic curves.
- Atkin and Morain – generalized this to all curves (fastest known program for “titanic” primes)
- In 2002 Agrawal, Kayal and Saxena gave a deterministic polynomial time algorithm (not using elliptic curves).

Shafi Goldwasser, Joe Kilian

Oliver Atkin

François Morain

Manindra Agrawal, Neeraj Kayal, Nitin Saxena

Why compute the Weil Pairing?

- Elliptic curve E/K, positive integer n, prime to char(K).
- A bilinear, alternating, galois equivariant, non-degenerate pairing $e_n : E[n] \times E[n] \to \mu_n$.
- It's used in descent calculations (a procedure to find a basis of the Mordell-Weil group).
- In that case n is usually quite small.
- What about when n is big?
- Schoof: can calculate $\#E(\mathbb{F}_p)$ quickly, what about the group structure?

Elliptic Curves and the Multiplicative Group

- In December 1984 I gave a talk at IBM about elliptic curve cryptography.
- Manuel Blum was in the audience, and challenged me to reduce ordinary discrete logs to elliptic curve discrete logs.
- Needed: an easily computable homomorphism from the multiplicative group to the elliptic curve group.
- The Weil pairing does relate them, if it could be computed quickly.
- But it went the wrong way!
- But – the degree of the extension field involved would almost always be as big as p (thus completely infeasible).

The Algorithm for the Weil Pairing

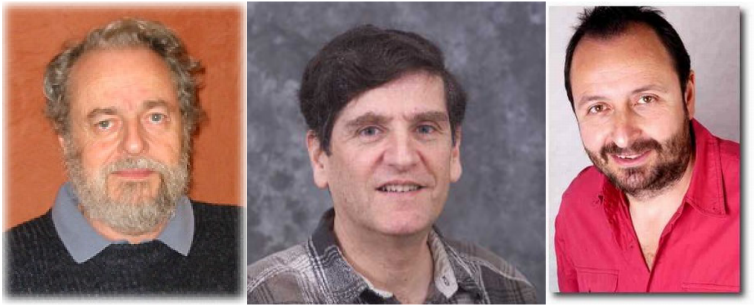
- Need to evaluate a function of very high degree at a selected point.
- In theory could use linear algebra – but dimension would be far too big – on the order of p.
- Used the process of quickly computing a multiple of a point to give an algorithm $O(\log p)$ operations in the field.
- Wrote up paper in late 1985.
- Widely circulated (and cited) as an unpublished manuscript.
- Expanded verison published in 2004 in J. Cryptology.

Manuel Blum

Group Structure

- As an abstract group $E(\mathbb{F}_p) \cong \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/de\mathbb{Z}$ for some positive integer d, e.
- Given $E/\mathbb{F}_p$ find d and e.
- By Schoof we can find $d^2e = \#E(\mathbb{F}_p)$ quickly.
- Weil pairing lets us find d and e.
- Above paper outlines how to do this.
- Needs to factor $\gcd(p-1, \#E(\mathbb{F}_p))$.
- Friedlander, Pomerance and Shparlinski analyze this latter problem.

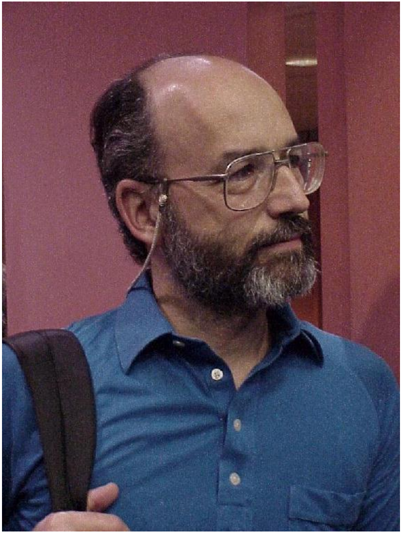
Friedlander, Pomerance and Shparlinski



The "Killer Application"?

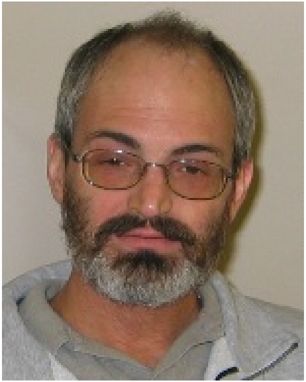
- In 1984 Adi Shamir proposed Identity Based Encryption – in which a public identity (such as an email address) could be used as a public key.
- In 2000, Antoine Joux gave the first steps toward realizing this as an efficient protocol using my Weil Pairing algorithm
- In 2001, Boneh and Franklin, gave the first fully functional version – also using the Weil pairing algorithm.
- It is now a burgeoning subfield – with thousands of papers.

Adi Shamir



Antoine Joux

Dan Boneh and Matt Franklin



Applications

- Elliptic Curve Cryptography is now used in many standards (IEEE, NIST, etc.).
- The NSA Information Assurance public web page has “The Case for Elliptic Curve Cryptography”
- Used in the Blackberry, Windows Media Player, standards for biometric data on passports, U. S. Federal Aviation Administration collision avoidance systems, and myriad others.

"How's everything?"

Alice and Bob